

ABELIAN p -EXTENSIONS AND ADDITIVE POLYNOMIALSJONNY FERNANDO BARRETO-CASTAÑEDA, FAUSTO JARQUÍN-ZÁRATE,
MARTHA RZEDOWSKI-CALDERÓN, AND GABRIEL VILLA-SALVADOR

ABSTRACT. In this work we present some arithmetic properties of families of abelian p -extensions of global function fields, among which are their generators and their type of ramification and decomposition.

1. INTRODUCTION

The study of elementary abelian p -extensions has been considered intensively by several authors. Usually, the way to study this type of extensions is to consider all its subextensions of degree p and then apply Hasse's criterion [2] as well as facts known about the behavior of the primes in these subextensions. Once this study has been done, one returns to the total extension. Garcia and Stichtenoth [1], changing the usual point of view, considered those extensions that can be given by a special type of additive polynomial; namely, the extensions given by an equation of the form $y^q - y = \alpha$. In their research, they obtained the genus of these extensions and used their results to build towers of function fields where the genus grows much faster than the number of rational points. In the same paper the authors mention that similar results can be obtained for additive polynomials having their roots in the base field.

In this paper we consider an additive polynomial $f(X)$ whose roots belong to the base field and we prove results analogous to the ones obtained by Garcia and Stichtenoth. For instance, given an additive polynomial, we show that any elementary abelian p -extension can be described by an equation of the type $f(X) = u$.

When the base field is a global rational function field, it is possible to give a lower bound for the ramification index of the ramified primes without considering its subextensions of degree p . It is also possible to characterize the fully decomposed primes. In the case of cyclic extensions of degree p given by an Artin-Schreier equation, the relation between two distinct generators is well known. In this article we give the corresponding result for elementary abelian p -extensions obtained by means of additive polynomials.

In the last part of this work, we generalize the results obtained to extensions which will be called *multicyclic*, and which are given by a Witt equation of the form $\bar{y}^q - \bar{y} = \bar{\alpha}$. Much of the formalism of the elementary abelian p -extensions can be translated to this new case and in fact it is possible to keep generalizing these results to other *additive vectorial polynomials* whose roots belong to the Witt

Date: June 7th., 2016.

2010 *Mathematics Subject Classification*. Primary 11R58; Secondary 11R60, 11R29.

Key words and phrases. Global function fields, ramification, elementary abelian p -extensions, Artin-Schreier extensions.

ring of the base field. In this paper we restrict ourselves to the case of an equation of the type $\vec{y}^q - \vec{y} = \vec{\alpha}$.

2. NOTATIONS

Let p a prime number, $n \in \mathbb{N}$ and $q = p^n$. Let k be an arbitrary field of characteristic p . When k is a function field, k_0 will denote the field of constants of k and we will assume that k_0 is a perfect field. Let $f(X) \in k[X]$ be an additive polynomial, that is, $f(x+y) = f(x) + f(y)$ for every $x, y \in \bar{k}$, a fixed algebraic closure of k . Then $f(X)$ is given by

$$(2.1) \quad f(X) = \sum_{i=0}^n a_i X^{p^i},$$

with $a_i \in k$. We will assume that f is monic and separable, that is, $a_n = 1$ and $a_0 \neq 0$. Furthermore, we will assume that the roots of $f(X)$ belong to the base field, that is,

$$(2.2) \quad \mathcal{G}_f := \{\xi \in \bar{k} \mid f(\xi) = 0\} \subseteq k.$$

As a special case, we will consider the additive polynomial $f(X) = X^{p^n} - X = X^q - X$.

In general, when we consider polynomials of the form $F(X) = f(X) - u \in k[X]$, we will assume that $F(X)$ is irreducible. Let $K = k(y)$ with $f(y) = u \in k$, that is, $F(y) = 0$. Then $f(y + \xi) = f(y) + f(\xi) = f(y) = u$ for all $\xi \in \mathcal{G}_f$ so that the set of roots of $F(X)$ is

$$y + \mathcal{G}_f = \{y + \xi \mid \xi \in \mathcal{G}_f\}.$$

We have that every element σ of $G = \text{Gal}(K/k)$ is determined by $\sigma(y)$. Since y and $\sigma(y)$ are conjugate, there exists $\xi_\sigma \in \mathcal{G}_f$ such that $\sigma(y) = y + \xi_\sigma$. From (2.2), we have that the extension $K = k(y)$ of k is a Galois extension of degree p^n .

Proposition 2.1. *In general, for any additive polynomial $f(X) \in k[X]$ of degree p^n , we have that \mathcal{G}_f is an additive group $\mathcal{G}_f \subseteq (\bar{k}, +)$ isomorphic to $C_p^n = (\mathbb{Z}/p\mathbb{Z})^n$. That is, \mathcal{G}_f is an \mathbb{F}_p -vector space of dimension n .*

Proof. For $\alpha, \beta \in \mathcal{G}_f$ we have

$$\begin{aligned} f(\alpha + \beta) &= f(\alpha) + f(\beta) = 0 + 0 = 0, \\ f(0) &= 0, \quad f(-\alpha) = f((p-1)\alpha) = \underbrace{f(\alpha) + \cdots + f(\alpha)}_{p-1} = 0 + \cdots + 0 = 0. \end{aligned}$$

Therefore $\mathcal{G}_f \subseteq (\bar{k}, +)$. Finally, $p\beta = 0$ for all $\beta \in \bar{k}$ and $|\mathcal{G}_f| = p^n$, so that $\mathcal{G}_f \cong C_p^n$. \square

In general, if V is a finite p -subgroup of k , then we denote:

$$f_V(X) = \prod_{\delta \in V} (X - \delta)$$

which is an additive polynomial ([7, proof of Proposition 13.4.10]). In particular an additive polynomial $f(X) \in k[X]$ (2.1) satisfies $f(X) = f_{\mathcal{G}_f}(X)$.

Proposition 2.2. *With the above notation, we have that $\theta: G \rightarrow \mathcal{G}_f$ given by $\theta(\sigma) = \xi_\sigma$, where $\sigma y = y + \xi_\sigma$, is a group monomorphism so that we may consider $G \subseteq \mathcal{G}_f$. When $F(X)$ is irreducible, we have the equality $G = \mathcal{G}_f$.*

Proof. For $\sigma, \tau \in G$, we have

$$y + \xi_{\sigma\tau} = \sigma\tau(y) = \sigma(y + \xi_\tau) = \sigma(y) + \xi_\tau = y + \xi_\sigma + \xi_\tau,$$

so that

$$\theta(\sigma\tau) = \xi_{\sigma\tau} = \xi_\sigma + \xi_\tau = \theta(\sigma) + \theta(\tau).$$

If $\theta(\sigma) = 0$, then $\sigma(y) = y$ which implies $\sigma = \text{Id}$. It follows that θ is a group monomorphism.

When $F(X)$ is irreducible, we have $|G| = [K : k] = \deg F(X) = p^n = |\mathcal{G}_f|$. \square

Remark 2.3. In case $\mathcal{G}_f \not\subseteq k$, we have that the decomposition field of $f(X)$ is $k(\mathcal{G}_f, y)$ and therefore $K = k(y)$ is not a normal extension of k . In fact we have $\text{Gal}(k(\mathcal{G}_f, y)/k) \cong \text{Gal}(k(\mathcal{G}_f)/k) \ltimes \text{Gal}(k(\mathcal{G}_f, y)/k(\mathcal{G}_f))$.

In general, if $\beta_1, \dots, \beta_m \in k$, $\mathcal{L}_{\mathbb{F}_p}\{\beta_1, \dots, \beta_m\}$ denotes the \mathbb{F}_p -vector space generated by β_1, \dots, β_m .

Finally, the Artin-Schreier operator is denoted by \wp , that is, $\wp(c) = c^p - c$ and \wp_a ($a \neq 0$) denotes the map $\wp_a(c) = c^p - a^{p-1}c = a^p \wp(\frac{c}{a})$. In case of a function field k/k_0 , with k_0 a finite field, R_T denotes the polynomial ring $k_0[T]$ and R_T^+ denotes the set of monic polynomials of $k_0[T]$.

The notation on Witt vectors will be given in Section 8.

3. THE POLYNOMIAL $X^q - X$

In [1] Garcia and Stichtenoth made a very thorough and complete study of extensions K/k when k is a function field, $K = k(y)$ with $y^q - y = u \in k$, $\mathbb{F}_q \subseteq k_0$ and they claim that analogous results hold for additive polynomials whose roots belong to k_0 . In this section we consider the case $f(X) = X^q - X \in k_0[X]$ and recall the main result of Garcia and Stichtenoth.

Proposition 3.1 (Garcia and Stichtenoth, [1]). *Assume that K/k is an elementary abelian p -extension of degree p^n and such that $\mathbb{F}_{p^n} \subseteq k_0$. Then, there exists $y \in K$ such that $K = k(y)$ whose minimal polynomial is $\text{Irr}(X, y, k) = X^{p^n} - X - a$ for some $a \in k$.*

Conversely, if $\mathbb{F}_{p^n} \subseteq k_0$ and $\varphi(X) = X^{p^n} - X - a \in k[X]$ is irreducible, then $K = k(y)$ with $\varphi(y) = 0$ is an elementary abelian p -extension of degree p^n . The intermediate fields $k \subseteq E_\mu \subseteq K$ of degree p over k , are given by $E_\mu = k(y_\mu)$ with $\mu \in \mathbb{F}_{p^n}^$ and*

$$y_\mu := (\mu y)^{p^{n-1}} + (\mu y)^{p^{n-2}} + \dots + (\mu y)^p + (\mu y),$$

$y_\mu^p - y_\mu = \mu a$; therefore $k(y) = k(\wp^{-1}(U))$ with $U = \{\mu a \mid \mu \in \mathbb{F}_{p^n}^\}$.* \square

Remark 3.2. Garcia and Stichtenoth claim that in Proposition 3.1 the polynomial $X^{p^n} - X$ can be replaced by any monic separable additive polynomial of degree p^n whose roots belong to k_0 and that an analogous description can be given for elementary abelian p -extensions. We will see this in Section 5.

4. GENERAL FACTS ON ELEMENTARY ABELIAN p -EXTENSIONS

For the time being we consider the special case of the polynomial $X^q - X$ with the notation and conventions of Section 2. Let k/k_0 be a function field, $G = \text{Gal}(K/k) \cong C_p^n$, $K = k(y)$, $y^q - y = u \in k$.

Theorem 4.1. *With the above notation, given a prime divisor \mathcal{P} of k , we have that there exists $y \in K$ such that $K = k(y)$, $y^q - y = u$ with $v_{\mathcal{P}}(u) \geq 0$ or $v_{\mathcal{P}}(u) = -\lambda p^m$ where $\lambda > 0$, $\gcd(\lambda, p) = 1$ and $0 \leq m < n$. If $v_{\mathcal{P}}(u) \geq 0$, \mathcal{P} is not ramified in K/k . If $v_{\mathcal{P}}(u) = -\lambda p^m$, then $p^{n-m} \mid e_{\mathcal{P}}$ where $e_{\mathcal{P}}$ denotes the ramification index of \mathcal{P} in K/k .*

Proof. See the proof of Theorem 5.2. \square

Remark 4.2. The number m given in Theorem 4.1 is not unique.

Example 4.3. Let $k = \mathbb{F}_q(T)$ with $\mathbb{F}_{p^2} \subseteq \mathbb{F}_q$ and let $K = k(y)$ where $y^{p^2} - y = u = T^{\lambda p}$ with $\lambda \in \mathbb{N}$, $\gcd(\lambda, p) = 1$. Then $v_{\mathcal{P}_{\infty}}(T) = -\lambda p$ and in this case $m = 1$, $n = 2$.

Set $z := y^p - T^{\lambda}$. Then

$$\begin{aligned} z^{p^2} - z &= (y^p)^{p^2} - (T^{\lambda})^{p^2} - y^p + T^{\lambda} = (y^{p^2} - y)^p - T^{\lambda p^2} + T^{\lambda} \\ &= (T^{\lambda p})^p - T^{\lambda p^2} + T^{\lambda} = T^{\lambda} = \nu, \end{aligned}$$

and in this case $v_{\mathcal{P}_{\infty}}(\nu) = -\lambda$, $m = 0$ and $n = 2$.

Note that necessarily $k(z) = k(y) = K$ since $e_{\mathcal{P}_{\infty}} = p^2 = [K : k]$. More generally, this is an immediate consequence of Theorem 7.2.

Definition 4.4. When a prime \mathcal{P} satisfies the conditions of Theorem 4.1 with respect to the equation $f(y) = u$, we say that is in a *normal form with respect to \mathcal{P}* . From Remark 4.2 we have that a normal form is not unique.

Remark 4.5. It does not hold necessarily that $e_{\mathcal{P}} = p^{n-m}$, see Example 4.3. In that example we have, with $m = 0$, $p^2 \mid e_{\mathcal{P}}$ and therefore $e_{\mathcal{P}} = p^2$. For $m = 1$, $p^{2-1} = p \mid e_{\mathcal{P}}$ but $e_{\mathcal{P}} \neq p$. Furthermore, even in case that m be the minimum with the previous properties or even in case that m is unique, it does not necessarily follow that $e_{\mathcal{P}} = p^{n-m}$. However, if $m = 0$, that is, if $v_{\mathcal{P}} = -\lambda$, then $p^n \mid e_{\mathcal{P}}$, thus $e_{\mathcal{P}} = p^n$ and the prime is fully ramified.

Example 4.6. Let $k = k_0(T)$ with $\mathbb{F}_{p^2} \subseteq k_0$. Let $K = k(y_1, y_2)$ with $y_1^p - y_1 = T$, $y_2^p - y_2 = T^2$ if $p > 2$ and $y_2^p - y_2 = T^3$ if $p = 2$. Then if $\mu \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, we consider $y = y_1 + \mu y_2$, and so we have $K = k(y)$ and

$$\begin{aligned} y^{p^2} - y &= y_1^{p^2} + \mu^{p^2} y_2^{p^2} - y_1 - \mu y_2 = (y_1^{p^2} - y_1) + \mu(y_2^{p^2} - y_2) \\ &= [(y_1^p - y_1)^p + (y_1^p - y_1)] + \mu[(y_2^p - y_2)^p + (y_2^p - y_2)] \\ &= T^p + T + \mu T^{2p} + \mu T^2 = T^p(1 + \mu T^p) + (T + \mu T^2) = \gamma, \end{aligned}$$

$$v_{\mathcal{P}_{\infty}}(\gamma) = -2p.$$

The other intermediate extensions K/k of degree p are given by $k(y_1 + \xi y_2)$, $1 \leq \xi \leq p-1$ and they satisfy

$$(y_1 + \xi y_2)^p - (y_1 + \xi y_2) = (y_1^p - y_1) + \xi(y_2^p - y_2) = T + \xi T^2,$$

$v_{\mathcal{P}_{\infty}}(T + \xi T^2) = -2$. In particular \mathcal{P}_{∞} is totally ramified, $e_{\mathcal{P}_{\infty}} = p^2$, $n = 2$, $m = 1$, $n - m = 1 < 2$.

Note that there is no way to obtain $m = 0$ with any change of variable because otherwise we would have $K = k(z)$ such that $z^{p^2} - z = \nu \in k$ and $v_{\mathcal{P}_\infty}(\nu) = -\lambda$ with $\gcd(\lambda, p) = 1$, and for any intermediate extension we would have

$$z_\mu^p - z_\mu = \mu\nu, \quad \nu \in \mathbb{F}_{p^2}^* \quad \text{and} \quad v_{\mathcal{P}_\infty}(\mu\nu) = -\lambda.$$

Therefore the different exponent of \mathfrak{p}_∞ , where \mathfrak{p}_∞ is a prime above \mathcal{P}_∞ , would be $(\lambda + 1)(p - 1)$ and $\lambda + 1$ would be the unique ramification number for all the intermediate extensions. However, in the subextensions $k(y_1)/k$ and $k(y_2)/k$ the ramification numbers are different, namely, $1 + 1 = 2$ and $2 + 1 = 3$ (or $3 + 1 = 4$ in case $p = 2$).

Therefore $m = 1$ is unique, $p^{n-m} = p^{2-1} = p \mid e_{\mathcal{P}_\infty}$ but $e_{\mathcal{P}_\infty} = p^2 \neq p$.

Example 4.7. Let $y_1^p - y_1 = T$, $y_2^p - y_2 = \frac{1}{T}$ and, $K = k(y_1, y_2)$. Then \mathcal{P}_∞ is not totally ramified since it is unramified in $k(y_2)/k$ and in this case $e_{\mathcal{P}_\infty} = p$, $n = 2$, $m = 1$ and $p^{n-m} = p = e_{\mathcal{P}_\infty}$.

5. ADDITIVE POLYNOMIALS

With the notation and conventions of Section 2, we consider $f(X) \in k[X]$ a monic separable additive polynomial of degree p^n :

$$(5.1) \quad f(X) = X^{p^n} + a_{n-1}X^{p^{n-1}} + \cdots + a_2X^{p^2} + a_1X^p + a_0X \in k[X], \quad a_0 \neq 0.$$

From Proposition 2.2 we know that \mathcal{G}_f is an additive group isomorphic to C_p^n with $\mathcal{G}_f \subseteq \bar{k}$, that is, $\mathcal{G}_f \subseteq (\bar{k}, +)$.

As always, we will assume that $\mathcal{G}_f \subseteq k$. Let $K = k(y)$ with $f(y) = u \in k$. We are assuming that $F(X) = f(X) - u \in k[X]$ is irreducible. Thus, from Proposition 2.2 we have that $G = \text{Gal}(K/k) \cong \mathcal{G}_f$.

Therefore, from Proposition 2.2, with $F(X)$ irreducible, we obtain that if the set $\{\varepsilon_1, \dots, \varepsilon_n\}$ is contained in \mathcal{G}_f then $\{\varepsilon_1, \dots, \varepsilon_n\}$ is a basis of \mathcal{G}_f over \mathbb{F}_p if and only if $G = \langle \sigma_{\varepsilon_1}, \dots, \sigma_{\varepsilon_n} \rangle$.

Now, G has $\frac{p^n-1}{p-1}$ subgroups of index p , that is, K/k has $\frac{p^n-1}{p-1}$ subextensions of degree p over k . We will study in more detail these subextensions.

If we denote by z the elements such that $k \subseteq k(z) \subseteq K$ with $[k(z) : k] = p$, then $k(z)$ is the fixed field of a subgroup H of G of index p : $k(z) = K^H$. In this case, if $G = H \oplus \mathbb{F}_p \sigma_z$, then $\text{Gal}(k(z)/k) \cong \langle \sigma_z \rangle$ with $\sigma_z(z) = z + 1$.

In this way we have that if $E = k(z_1, \dots, z_n)$, then $E = K$ if and only if $G = \langle \sigma_{z_1}, \dots, \sigma_{z_n} \rangle$. Now, let $K = k(z_1, \dots, z_n)$ and denote $\text{Gal}(k(z_i)/k) = \langle \sigma_i \rangle$ and $G \cong \langle \sigma_1, \dots, \sigma_n \rangle$. Set $z := \alpha_1 z_1 + \cdots + \alpha_n z_n$ with $\alpha_1, \dots, \alpha_n \in \mathbb{F}_p$ not all zero. Then if $\wp(z_i) = z_i^p - z_i = \gamma_i$, we have

$$z^p - z = \wp(z) = \wp\left(\sum_{i=1}^n \alpha_i z_i\right) = \sum_{i=1}^n \alpha_i \wp(z_i) = \sum_{i=1}^n \alpha_i \gamma_i.$$

Note that $\{\gamma_1, \dots, \gamma_n\} \subseteq k$ is linearly independent over \mathbb{F}_p since otherwise, if $\sum_{i=1}^n \alpha_i \gamma_i = 0$ with some $\alpha_{i_0} \neq 0$, then $\gamma_{i_0} = \sum_{i \neq i_0} \alpha_i^{-1} \alpha_i \gamma_i$ so that

$$\wp(z_{i_0}) = z_{i_0}^p - z_{i_0} = \gamma_{i_0} = \sum_{i \neq i_0} \alpha_{i_0}^{-1} \alpha_i \gamma_i = \sum_{i \neq i_0} \alpha_{i_0}^{-1} \alpha_i (z_i^p - z_i) = \wp\left(\sum_{i \neq i_0} \alpha_{i_0}^{-1} \alpha_i z_i\right),$$

which implies that

$$\wp(z_{i_0} - \sum_{i \neq i_0} \alpha_{i_0}^{-1} \alpha_i z_i) = 0.$$

Hence $z_{i_0} - \sum_{i \neq i_0} \alpha_{i_0}^{-1} \alpha_i z_i = \beta \in \mathbb{F}_p$. It follows that

$$z_{i_0} \in k(z_1, \dots, z_{i_0-1}, z_{i_0+1}, \dots, z_n) \quad \text{and that} \quad [K : k] \leq p^{n-1},$$

which is absurd. In this way we have that $\{\gamma_1, \dots, \gamma_n\} \subseteq k$ is a set linearly independent over \mathbb{F}_p .

Coming back to the expression $z = \sum_{i=1}^n \alpha_i z_i$, we have $\wp(z) = \sum_{i=1}^n \alpha_i \gamma_i = \gamma$. In case $\gamma \in \wp(k)$, say $\gamma = \wp(A)$ with $A \in k$, we would have $\wp(z - A) = \wp(\sum_{i=1}^n \alpha_i z_i - A) = 0$. Therefore $\sum_{i=1}^n \alpha_i z_i - A = \beta \in \mathbb{F}_p$. Because $\alpha_{i_0} \neq 0$, it would follow that

$$z_{i_0} = - \sum_{i \neq i_0} \alpha_{i_0}^{-1} \alpha_i z_i + \alpha_{i_0}^{-1} \beta + \alpha_{i_0} A \in k(z_1, \dots, z_{i_0-1}, z_{i_0+1}, \dots, z_n),$$

which is absurd. Whence $\gamma \notin \wp(k)$ and $[k(z) : k] = p$.

With this procedure we obtain $p^n - 1$ extensions of degree p . Now, if $k(z) = k(w)$ with $z = \sum_{i=1}^n \alpha_i z_i$ and $w = \sum_{i=1}^n \beta_i z_i$, $\alpha_i, \beta_i \in \mathbb{F}_p$, it follows that $z = jw + c$ (see Proposition 7.1) with $j \in \mathbb{F}_p^*$ and $c \in k$. Therefore $c = 0$ and $z = jw$. Hence we obtain $\frac{p^n-1}{p-1}$ different extensions of degree p , hence all of them. In brief, we have obtained

Proposition 5.1. *If $K = k(z_1, \dots, z_n)/k$ is an elementary abelian p -extension of degree p^n and $[k(z_i) : k] = p$, $1 \leq i \leq n$, then all the subextensions of degree p over k are given by $k(z)$ where $z = \alpha_1 z_1 + \dots + \alpha_n z_n$ with $\alpha_1, \dots, \alpha_n \in \mathbb{F}_p$ not all zero.* \square

Now consider k/k_0 a function field with k_0 a perfect field, $f(X) \in k_0[X]$ and $\mathcal{G}_f \subseteq k_0$. Let $f(X)$ be given by (5.1). Let $K = k(y)$ with $f(y) = u \in k$. Let \mathcal{P} be a place of k . We have the same result as in Theorem 4.1, namely:

Theorem 5.2. *We can choose $u \in k$ such that, either $v_{\mathcal{P}}(u) \geq 0$ or $v_{\mathcal{P}}(u) = -\lambda p^m$ with $\lambda \in \mathbb{N}$, $\gcd(\lambda, p) = 1$ and $0 \leq m < n$. In the first case \mathcal{P} is unramified in K/k and in the second \mathcal{P} is ramified and $p^{n-m} \mid e_{\mathcal{P}}$.*

Proof. Later on (Theorem 5.5) we will see how to obtain all the degree p subextensions. Once we have these subextensions we may use them to determine the decomposition type of \mathcal{P} . Here we present another proof in the spirit of Hasse's for Artin-Schreier extensions [2].

(1) If $v_{\mathcal{P}}(u) \geq 0$, then $u \in \mathcal{O}_{\mathcal{P}}$. With $f(y) = u$, if we define $h(X) = \text{Irr}(X, y, k)$, we obtain that $h(X) \mid f(X) - u$. Therefore $f(X) - u = h(X)l(X)$ and $f'(X) = h'(X)l(X) + h(X)l'(X)$. It follows that $f'(y) = h'(y)l(y) + 0$. In this way we obtain $h'(y) \mid f'(y)$.

Now, if $y \in \mathcal{O}_{\mathfrak{p}}$ where \mathfrak{p} is a prime divisor of K over \mathcal{P} , $f'(y) = a_0 \neq 0$, $v_{\mathcal{P}}(a_0) = 0$ since $a_0 \in k_0^*$. Therefore, the local different satisfies $\mathfrak{D}_{\mathcal{O}_{\mathfrak{p}}/\mathcal{O}_{\mathcal{P}}} \mid \langle f'(y) \rangle = \{1\}$. Hence $\mathfrak{p} \nmid \mathfrak{D}_{K/k}$ and \mathfrak{p} is unramified.

(2) If $v_{\mathcal{P}}(u) < 0$, let $v_{\mathcal{P}}(u) = -\lambda p^m$. If $m < n$, u satisfies the conditions of the theorem. If $m \geq n$, we set $\lambda p^m = \lambda_1 p^n$, $u \in k \subseteq k_{\mathcal{P}}$ and π a prime element for \mathcal{P} ,

$v_{\mathcal{P}}(\pi) = 1, \pi \in k$. Write u in the form

$$(5.2) \quad u = \frac{b_{-\lambda p^m}}{\pi^{\lambda p^m}} + \frac{b_{-\lambda p^m+1}}{\pi^{\lambda p^m-1}} + \cdots + \frac{b_{-1}}{\pi} + b_0 + b_1 \pi + \cdots \in k_{\mathcal{P}} \cong k(\mathcal{P})((\pi)).$$

There exists $c \in k(\mathcal{P})$ such that $c^{p^n} = b_{-\lambda_1 p^n}$. Let $C \in \mathcal{O}_{\mathcal{P}}$ where $k(\mathcal{P}) = \mathcal{O}_{\mathcal{P}}/\mathcal{P}$, be such that $c = C \bmod \mathcal{P} \in k(\mathcal{P})$. Set $z = y - C\pi^{-\lambda_1}$. Then $k(z) = k(y) = K$ and

$$\begin{aligned} f(z) &= f(y) - f(C\pi^{-\lambda_1}) \\ &= u - (C^{p^n} \pi^{-\lambda_1 p^n} + a_{n-1} C^{p^{n-1}} \pi^{-\lambda_1 p^{n-1}} + \cdots + a_1 C^p \pi^{-\lambda_1 p} + a_0 C \pi^{-\lambda_1}) \\ &= \frac{b_{-\lambda p^m}}{\pi^{\lambda p^m}} + \frac{b_{-\lambda p^m+1}}{\pi^{\lambda p^m-1}} + \cdots + \frac{b_{-1}}{\pi} + b_0 + b_1 \pi + \cdots \\ &\quad - \left(\frac{b_{-\lambda p^m}}{\pi^{\lambda p^m}} + \frac{d_{-\lambda p^m+1}}{\pi^{\lambda p^m-1}} + \cdots + \frac{d_{-\lambda_1}}{\pi^{\lambda_1}} \right) \\ &= \sum_{i \geq -\lambda p^m+1} \gamma_i \pi^i, \quad \gamma_i \in k(\mathcal{P}). \end{aligned}$$

Therefore $v_{\mathcal{P}}(u - f(C\pi^{-\lambda p^m})) \geq -\lambda p^m + 1 > -\lambda p^m$. In brief, if $v_{\mathcal{P}}(u) = -\lambda p^m$ with $m \geq n$, there exists $\delta \in k$ such that if $z := y - \delta$, then $k(z) = k(y)$ and $v_{\mathcal{P}}(u - f(\delta)) > -\lambda p^m$.

With this procedure we can reduce to an equation $f(y) = u$ with $v_{\mathcal{P}}(u) \geq 0$ or $v_{\mathcal{P}}(u) = -\lambda p^m$, $\gcd(\lambda, p) = 1$, $\lambda > 0$ and $0 \leq m < n$. This finishes the process.

If u is of this last form, we will see that for every $\delta \in k$, $v_{\mathcal{P}}(u - f(\delta)) \leq v_{\mathcal{P}}(u)$, that is, the value of $v_{\mathcal{P}}(u)$ is the maximum possible with substitutions of the type $z = y - \delta$ with $\delta \in k$. We have $f(\delta) = \delta^{p^n} + a_{n-1} \delta^{p^{n-1}} + \cdots + a_1 \delta^p + a_0 \delta$.

In case $v_{\mathcal{P}}(\delta) \geq 0$, $v_{\mathcal{P}}(f(\delta)) \geq 0$ and since $v_{\mathcal{P}}(u) < 0$, it follows that

$$v_{\mathcal{P}}(u - f(\delta)) = \min\{v_{\mathcal{P}}(u), v_{\mathcal{P}}(f(\delta))\} = v_{\mathcal{P}}(u).$$

In case $v_{\mathcal{P}}(\delta) < 0$, $v(\delta^{p^n}) = p^n v_{\mathcal{P}}(\delta) < p^i v_{\mathcal{P}}(\delta) \leq v_{\mathcal{P}}(a_i) + p^i v_{\mathcal{P}}(\delta) = v_{\mathcal{P}}(a_i \delta^{p^i})$. Therefore $v_{\mathcal{P}}(f(\delta)) = p^n v_{\mathcal{P}}(\delta) = v_{\mathcal{P}}(\delta^{p^n})$. Now $v_{\mathcal{P}}(f(\delta)) \equiv 0 \bmod p^n$ and $v_{\mathcal{P}}(u) \not\equiv 0 \bmod p^n$. Thus $v_{\mathcal{P}}(f(\delta)) \neq v_{\mathcal{P}}(u)$ and $v_{\mathcal{P}}(u - f(\delta)) = \min\{v_{\mathcal{P}}(u), v_{\mathcal{P}}(f(\delta))\} \leq v_{\mathcal{P}}(u)$.

Let \mathfrak{p} be a place of K above \mathcal{P} . Then $v_{\mathfrak{p}}(y) < 0$ and hence $v_{\mathfrak{p}}(f(y)) = p^n v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(y^{p^n})$. Therefore $v_{\mathfrak{p}}(f(y)) = p^n v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(u) = e_{\mathcal{P}} v_{\mathcal{P}}(u) = -e_{\mathcal{P}} \lambda p^m$ and it follows that $p^{n-m} \mid e_{\mathcal{P}}$ since $\gcd(\lambda, p) = 1$. \square

When u is written with respect to a prime divisor \mathcal{P} as in Theorem 5.2, we say that u is in a *normal form with respect to \mathcal{P}* . A normal form is not unique in general.

In case $k = k_0(T)$ is a rational function field and $\mathcal{G}_f \subseteq k_0$ we have:

Theorem 5.3. *Let $k = k_0(T)$ be a rational function field, $f(X) \in k_0[X]$ an additive polynomial given by (5.1) and $K = k(y)$ an elementary abelian p -extension where $f(y) = u \in k$ and $F(X) = f(X) - u \in k[X]$ is irreducible of degree p^n . Then we can choose u satisfying*

$$(5.3) \quad u = \sum_{i=1}^r \frac{Q_i(T)}{P_i(T)^{\alpha_i}} + R(T)$$

where P_1, \dots, P_r are distinct monic irreducible polynomials, $Q_1, \dots, Q_r \in k_0[T]$ such that $\gcd(Q_i, P_i) = 1$, $\deg Q_i < \deg P_i^{\alpha_i}$, $\alpha_i = -\lambda_i p^{m_i} > 0$ with $0 \leq m_i < n$ and $\gcd(\lambda_i, p) = 1$ for $1 \leq i \leq r$ and $R(T)$ is a polynomial such that if $R(T) \notin k_0$ then

$\deg R(T) = \lambda_0 p^m > 0$ with $\gcd(\lambda_0, p) = 1$, $0 \leq m < n$ and if $R(T) \in k_0$ then either $R(T) = 0$ or $R(T) \notin f(k_0) = \{f(\delta) \mid \delta \in k_0\}$.

Furthermore P_1, \dots, P_r are precisely the finite prime divisors of k ramified in K and \mathcal{P}_∞ is ramified if and only if $R(T) \notin k_0$.

Proof. Let $f(y) = u = \frac{g(T)}{h(T)}$ with $\gcd(g(T), h(T)) = 1$. Expanding in partial fractions, we obtain

$$u = \sum_{i=1}^r \sum_{j=1}^{\beta_i} \frac{Q_j^{(i)}(T)}{P_i(T)^j} + R(T),$$

where $\deg Q_j^{(i)} < \deg P_i^j$ for any $1 \leq j \leq \beta_i$, $1 \leq i \leq r$ and $R(T) \in k_0[T]$.

If $\beta_1 = \lambda p^n > 0$, we can choose $C \in k[T]$ such that

$$C(T)^{p^n} \equiv Q_1^{(\beta_1)}(T) \pmod{P_1(T)}$$

because $k_0[T]/(P_1)$ is a perfect field. Using the substitution $z = y - C^\lambda$ we get $K = k(z)$ and $f(z) = f(y) - f(C^\lambda) = u - f(C^\lambda) = w$. It follows that the valuations of w for an arbitrary prime divisor $\mathcal{P} \neq \mathcal{P}_\infty$ of k_0 satisfy:

$$v_{\mathcal{P}}(w) \begin{cases} \geq 0 & \text{if } v_{\mathcal{P}}(u) \geq 0 \\ = -\beta_j & \text{if } \mathcal{P} \text{ is the prime divisor associated to } P_j(T) \text{ for } 2 \leq j \leq r \\ > -\beta_1 & \text{if } \mathcal{P} \text{ is the prime divisor associated to } P_1(T). \end{cases}$$

Repeating this process, we obtain, for β_j , $2 \leq j \leq r$, that $K = k(y)$ with $f(y) = u$ and u is in the form (5.3) except possibly for $R(T)$.

Now if $R(T) = b_d T^d + \dots + d_0$ satisfies $d = \lambda p^n$ we make the substitution $y = z - cT^\lambda$ where $c^{p^n} = b_d$. Keeping on this process we finally obtain that either $R(T) \in k_0$ or $\deg R(T) = \lambda p^m$ with $0 \leq m < n$. Finally, if $R(T) \in k_0$ and $R(T) = f(\delta)$ for some $\delta \in k_0$, we take $z = y - \delta$.

The type of ramification is an immediate consequence of Theorem 5.2. \square

Definition 5.4. When the equation $f(y) = u$ defining the extension $K = k(y)$ satisfies the conditions of Theorem 5.3, we say that the equation is in a *reduced form*.

Note that the reduced form is not unique in general.

Next, we present the results mentioned by Garcia and Stichtenoth [1] on additive polynomials whose roots belong to the base field.

Let $K = k(y)$ with $f(y) = u \in k$, $f(X) \in k[X]$ a monic separable additive polynomial whose roots are in k and $F(X) = f(X) - u \in k[X]$ is irreducible, $G = \text{Gal}(K/k) \cong \mathcal{G}_f \cong C_p^n$.

Theorem 5.5. The subextensions of degree p over k of K/k are given by $k(z_{\mathcal{H}})$ with

$$z_{\mathcal{H}}^p - z_{\mathcal{H}} = \frac{u}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p},$$

where $\mathcal{H} < \mathcal{G}_f$ is a subspace of \mathcal{G}_f of codimension 1, $f_{\mathcal{H}}(X) = \prod_{\delta \in \mathcal{H}} (X - \delta)$ and $\mathcal{G}_f = \mathcal{H} + \mathbb{F}_p \varepsilon_{\mathcal{H}}$, $\varepsilon_{\mathcal{H}} \in \mathcal{G}_f$. Furthermore, $k(z_{\mathcal{H}})$ is the fixed field under \mathcal{H} : $k(z_{\mathcal{H}}) = K^{\mathcal{H}}$ and $\text{Gal}(k(z_{\mathcal{H}})/k) = \langle \sigma_{\varepsilon_{\mathcal{H}}} \rangle$ where $\sigma_{\varepsilon_{\mathcal{H}}}(y) = y + \varepsilon_{\mathcal{H}}$. We have $\sigma_{\varepsilon_{\mathcal{H}}}(z_{\mathcal{H}}) = z_{\mathcal{H}} + 1$.

Proof. We have $f(X) = \prod_{\alpha \in \mathbb{F}_p} f_{\mathcal{H}}(X - \alpha \varepsilon_{\mathcal{H}})$. Now, $f_{\mathcal{H}}(X)$ is an additive polynomial (see for instance [7, proof of Proposition 13.4.10]) and $f_{\mathcal{H}}(X - \alpha \varepsilon_{\mathcal{H}}) = f_{\mathcal{H}}(X) - \alpha f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})$.

Denote $Y := f_{\mathcal{H}}(X)$. Then

$$\begin{aligned} f(X) &= \prod_{\alpha=0}^{p-1} (Y - \alpha f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})) = f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p \cdot \prod_{\alpha=0}^{p-1} \left(\frac{Y}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} - \alpha \right) \\ &= f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p \left(\left(\frac{Y}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} \right)^p - \frac{Y}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} \right). \end{aligned}$$

So,

$$f(X) = f_{\mathcal{H}}(X)^p - f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^{p-1} f_{\mathcal{H}}(X) = f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p \left(\left(\frac{f_{\mathcal{H}}(X)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} \right)^p - \left(\frac{f_{\mathcal{H}}(X)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} \right) \right).$$

That is,

$$f(X) = f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p \wp \left(\frac{f_{\mathcal{H}}(X)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} \right) = \wp_{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})}(f_{\mathcal{H}}(X)).$$

In this way we obtain $f(X) = f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p (z^p - z)$ where $z = \frac{Y}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} = \frac{f_{\mathcal{H}}(X)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})}$. Let

$$(5.4) \quad z_{\mathcal{H}} := \frac{f_{\mathcal{H}}(y)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})}.$$

Then

$$z_{\mathcal{H}}^p - z_{\mathcal{H}} = \frac{f(y)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p} = \frac{u}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p} \quad \text{or} \quad \wp_{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})}(f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})z_{\mathcal{H}}) = u.$$

Furthermore, if the set $\{\varepsilon_1, \dots, \varepsilon_{n-1}\}$ is an \mathbb{F}_p -basis of \mathcal{H} and $\varepsilon_n := \varepsilon_{\mathcal{H}}$, then $\{\varepsilon_1, \dots, \varepsilon_{n-1}, \varepsilon_n\}$ is a basis of \mathcal{G}_f over \mathbb{F}_p . We have that if $\sigma_{\varepsilon_i}(y) = y + \varepsilon_i$, then $G = \langle \sigma_{\varepsilon_1}, \dots, \sigma_{\varepsilon_{n-1}}, \sigma_{\varepsilon_n} \rangle$ and we have, for $1 \leq i \leq n-1$,

$$\sigma_{\varepsilon_i}(z_{\mathcal{H}}) = \sigma_{\varepsilon_i} \left(\frac{f_{\mathcal{H}}(y)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} \right) = \frac{f_{\mathcal{H}}(y + \varepsilon_i)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} = \frac{f_{\mathcal{H}}(y) + f_{\mathcal{H}}(\varepsilon_i)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} = \frac{f_{\mathcal{H}}(y) + 0}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})} = z_{\mathcal{H}},$$

and

$$\sigma_{\varepsilon_n}(z_{\mathcal{H}}) = \frac{f_{\mathcal{H}}(y + \varepsilon_n)}{f_{\mathcal{H}}(\varepsilon_n)} = z_{\mathcal{H}} + 1,$$

so that $k(z_{\mathcal{H}})/k$ is a subextension of K/k of degree p , the field $k(z_{\mathcal{H}})$ is the fixed field under \mathcal{H} and $\text{Gal}(k(z_{\mathcal{H}})/k) \cong \langle \sigma_{\varepsilon_n} \rangle$ where $\sigma_{\varepsilon_n}(y) = y + \varepsilon_{\mathcal{H}}$. \square

Remark 5.6. Theorem 5.5 must be compared with Theorem 7.3 which is more general but less explicit.

Theorem 5.7. Let $f(X) \in k[X]$ be a monic separable additive polynomial of degree p^n with $\mathcal{G}_f \subseteq k$. Let K/k be an elementary abelian p -extension of degree p^n . Then there exist $y \in K$ and $u \in k$ such that $K = k(y)$ and $f(y) = u$.

Proof. Let $y_1, \dots, y_n \in K$ be such that $K = k(y_1, \dots, y_n)$ and $y_i^p - y_i = \gamma_i \in k$. Let $G = \text{Gal}(K/k)$, $G = \langle \sigma_1, \dots, \sigma_n \rangle$ with $\sigma_i(y_j) = y_j + \delta_{ij}$ where δ_{ij} is the Kronecker delta. Let $\{\mu_1, \dots, \mu_n\}$ be a basis of \mathcal{G}_f over \mathbb{F}_p . Let $y := \sum_{i=1}^n \mu_i y_i$ and let $f(X)$ be given as in (5.1).

We have $y_i^p = y_i + \gamma_i$, $y_i^{p^2} = y_i^p + \gamma_i^p = y_i + \gamma_i + \gamma_i^p$ and in general $y_i^{p^m} = y_i + l_m(\gamma_i)$ where $l_m(\gamma_i) = \gamma_i + \gamma_i^p + \cdots + \gamma_i^{p^{m-1}}$, $m \in \mathbb{N}$. Then

$$f(\mu_i y_i) = \sum_{j=0}^n a_j (\mu_i y_i)^{p^j} = \sum_{j=0}^n a_j (\mu_i^{p^j} y_i + \mu_i^{p^j} l_j(\gamma_i)) = y_i f(\mu_i) + h_i,$$

with $h_i = \sum_{j=0}^n a_j \mu_i^{p^j} l_j(\gamma_i)$ and $y_i f(\mu_i) = 0$ because $\mu_i \in \mathcal{G}_f$. Therefore,

$$f(y) = f\left(\sum_{i=1}^n \mu_i y_i\right) = \sum_{i=1}^n f(\mu_i y_i) = \sum_{i=1}^n h_i = u \in k.$$

If $\sigma \in G$, there exist $\nu_1, \dots, \nu_n \in \mathbb{F}_p$ such that $\sigma = \sigma_1^{\nu_1} \cdots \sigma_n^{\nu_n}$ and

$$\sigma(y) = \sigma\left(\sum_{i=1}^n \mu_i y_i\right) = \sum_{i=1}^n \mu_i (y_i + \nu_i) = y + \sum_{i=1}^n \nu_i \mu_i.$$

Thus $\sigma = \text{Id} \iff \sigma(y) = y \iff \sum_{i=1}^n \nu_i \mu_i = 0 \iff \nu_1 = \cdots = \nu_n = 0$, confirming that $\{\mu_1, \dots, \mu_n\}$ is a basis of \mathcal{G}_f over \mathbb{F}_p and that $G = \text{Gal}(K/k) = \langle \sigma_1, \dots, \sigma_n \rangle$. \square

6. DECOMPOSITION OF PRIME DIVISORS IN ELEMENTARY ABELIAN p -EXTENSIONS OF FUNCTION FIELDS

Let us to consider $k = k_0(T)$ a rational function field where we assume that k_0 is a finite field with $\mathcal{G}_f \subseteq k_0$. The aim of this section is to describe the decomposition of the unramified primes in an elementary abelian p -extension K of k given by $K = k(y)$ where $f(y) = u$, $f(X) \in k_0[X]$ given by (5.1) and such that $\mathcal{G}_f \subseteq k_0$. Note that the decomposition group of any unramified prime is a cyclic group and therefore it is of order 1 or p . We will assume that the extension K/k is geometric.

A fundamental result that we will use in this section is the decomposition of \mathcal{P}_∞ in Artin-Schreier extensions.

Proposition 6.1. *Let L/K be a cyclic extension of degree p such that $K = k(w)$ with $w \in L$ given in the form*

$$(6.1) \quad w^p - w = u = \sum_{i=1}^r \frac{Q_i}{P_i^{e_i}} + f(T) = \frac{Q}{P_1^{e_1} \cdots P_r^{e_r}} + f(T),$$

where $P_i \in R_T^+$, $Q_i \in R_T$, $\gcd(P_i, Q_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\deg Q_i < \deg P_i^{e_i}$, $1 \leq i \leq r$, $\deg Q < \sum_{i=1}^r \deg P_i^{e_i}$, $f(T) \in R_T$, with $p \nmid \deg f$ in case $f(T) \notin k_0$ and $f(T) \notin \wp(k_0)$ when $f(T) \in k_0^*$. Then the prime divisor \mathcal{P}_∞ is

- (a).- decomposed if $f(T) = 0$.
- (b).- inert if $f(T) \in k_0$ and $f(T) \notin \wp(k_0)$.
- (c).- ramified if $f(T) \notin k_0$ (so that $p \nmid \deg f$).

\square

The following example illustrates several of the results obtained.

Example 6.2. Let $k = \mathbb{F}_{27}(T)$ and $K = k(z)/k$ be the 3-elementary abelian extension of degree 27, defined by the equation:

$$z^{27} - z = \frac{1}{(T+1)^{54}} + \frac{1}{T+1} + T^9 + T^3 + T + \omega + 1 = u(T),$$

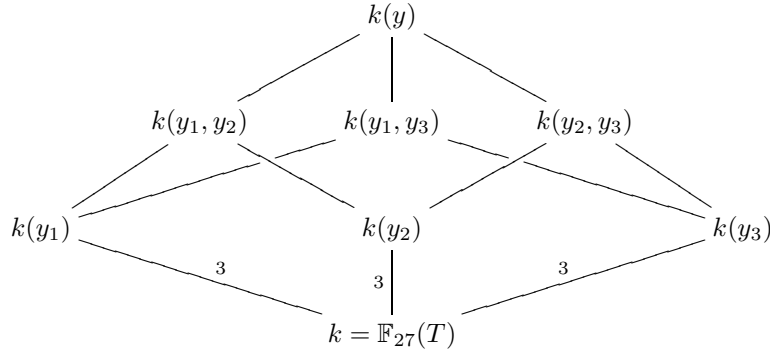
where $\omega \in \mathbb{F}_{27}$, $\omega^3 = \omega + 2$ and $\mathbb{F}_{27} = \mathbb{F}_3(\omega)$. First, note that if $y = z - \frac{1}{(T+1)^2}$, then $k(y) = k(z)$ and $y^{27} - y = (z - \frac{1}{(T+1)^2})^{27} - (z - \frac{1}{(T+1)^2}) = u(T) - \frac{1}{(T+1)^{54}} + \frac{1}{(T+1)^2}$. That is

$$y^{27} - y = \frac{1}{(T+1)^2} + \frac{1}{T+1} + T^9 + T^3 + T + \omega + 1 = r(T).$$

From Theorem 4.1, the prime divisor \mathcal{P}_1 , associated to the irreducible polynomial $p_1(T) = T + 1$ and \mathcal{P}_∞ , are ramified. Next, we compute the ramification index for these prime divisors. We can use Proposition 3.1 to obtain all the $13 = \frac{3^3-1}{3-1}$ Artin-Schreier subextensions. Three of these extensions that generate the whole extension are given by:

$$\begin{aligned} y_1^3 - y_1 &= r(T), \\ y_1 &= y^9 + y^3 + y, \\ y_2^3 - y_2 &= \omega r(T), \\ y_2 &= (\omega y)^9 + (\omega y)^3 + \omega y, \\ y_3^3 - y_3 &= \omega^2 r(T), \\ y_3 &= (\omega^2 y)^9 + (\omega^2 y)^3 + \omega^2 y. \end{aligned}$$

The following diagram represents these 3-subextensions and some elementary abelian 3-extensions of degree 9.



Note that \mathcal{P}_1 is fully ramified, that is $e(\wp_1|\mathcal{P}_1) = 27$ for a place \wp_1 above \mathcal{P}_1 , since $v_{\mathcal{P}_1}(r(T)) = -2$ is relatively prime to 3. On the other hand, if $z_{1,1} = y_1 - T^3$, then $k(z_{1,1}) = k(y_1)$ and $z_{1,1}^3 - z_{1,1} = \frac{1}{(T+1)^2} + \frac{1}{T+1} + 2T^3 + T + \omega + 1$. Now, let $z_{1,2} = z_{1,1} + T - \omega^2$. We have $k(z_{1,2}) = k(z_{1,1}) = k(y_1)$ and

$$z_{1,2}^3 - z_{1,2} = \frac{1}{(T+1)^2} + \frac{1}{T+1} = r_1(T).$$

From Proposition 6.1, \mathcal{P}_∞ decomposes in $k(y_1)/k$.

In the extension $k(y_2)/k$, we let $z_{2,1} = y_2 + (2\omega + 2)T^3$. Then $k(z_{2,1}) = k(y_2)$ and $z_{2,1}^3 - z_{2,1} = (2\omega + 1)T^3 + \omega T + \omega^2 + \omega + \frac{\omega}{(T+1)^2} + \frac{\omega}{T+1}$. Again, if we make the substitution: $z_{2,2} = z_{2,1} - 2\omega T$, in this extension, we obtain $k(z_{2,2}) = k(z_{2,1}) = k(y_2)$ and

$$z_{2,2}^3 - z_{2,2} = \frac{\omega}{(T+1)^2} + \frac{\omega}{T+1} + \omega^2 + \omega = r_2(T),$$

because $\omega^2 + \omega \notin \wp(\mathbb{F}_{27})$, from Proposition 6.1 it follows that the infinite prime is inert in $k(y_2)/k$. Finally, with the substitutions: $z_{3,1} = y_3 - (2\omega^2 + \omega + 2)T^3$ and $z_{3,2} = z_{3,1} - (2\omega^2 + 2)T$, we obtain $k(z_{3,2}) = k(z_{3,1}) = k(y_3)$, where

$$z_{3,2}^3 - z_{3,2} = \frac{\omega^2}{(T+1)^2} + \frac{\omega^2}{T+1} + 2T + \omega^2 + \omega + 2 = r_3(T).$$

Therefore, \mathcal{P}_∞ is ramified in $k(y_3)/k$. Hence, the decomposition field of the infinite prime \mathcal{P}_∞ is $k(y_2)$ and the inertia field is $k(y_2, y_3)$. We obtain \mathcal{P}_∞ has ramification index equal to 3, inertia degree equal to 3 and has 3 prime divisors in K above it.

Returning to our study, note that with the hypothesis of being of degree p , separable and with the roots in the base field, essentially there is a unique additive polynomial of degree p . If $X^p + aX$ is an additive polynomial, their roots are equal to $i\alpha$ with $0 \leq i \leq p-1$ and $\alpha = \sqrt[p-1]{-a}$ a fixed nonzero root of $X^p + aX$. We are assuming that $\alpha \in k_0^*$. Then $\alpha^p = -\alpha a$ and

$$X^p + aX = \alpha^p(Z^p - Z) \quad \text{with} \quad Z = \frac{X}{\alpha}, \quad \alpha \in \mathbb{F}_q^*,$$

that is, $X^p + aX = \alpha^p \wp(\frac{X}{\alpha})$ with $\alpha^{p-1} = -a$.

We come back to the extension $K = k(y)$, $\text{Gal}(K/k) \cong \mathcal{G}_f$. We have that the decomposition of \mathcal{P}_∞ in K , in case of being unramified is

Proposition 6.3. *Let $K = k(y)/k$ with $f(y) = u$ and u given in a reduced form (5.3). We assume that \mathcal{P}_∞ is unramified in K/k . If $R(T) = 0$, then \mathcal{P}_∞ decomposes fully in K/k . Conversely, if \mathcal{P}_∞ decomposes fully, then there exists a reduced form $f(y) = u$ where $R(T) = 0$.*

Proof. If $R(T) = 0$ then, from Theorem 5.5 and Proposition 6.1, it follows that \mathcal{P}_∞ decomposes in every subextension of degree p and therefore \mathcal{P}_∞ is fully decomposed in K/k .

Conversely, assume that \mathcal{P}_∞ is fully decomposed. Let $K = k(y_1, \dots, y_n)$ with $k(y_i)/k$ cyclic extensions of degree p given by Artin-Schreier equations in reduced form. Since \mathcal{P}_∞ decomposes in all of them, from Theorem 5.7, it follows $K = k(y_0)$ with $y_0 = \sum_{i=1}^n \mu_i y_i$, $\{\mu_1, \dots, \mu_n\}$ a basis of \mathcal{G}_f over \mathbb{F}_p , and in the reduced form of $f(y_0) = u_0$, the polynomial corresponding to the behavior of \mathcal{P}_∞ is 0. \square

In the special case of the additive polynomial $f(X) = X^q - X$, we are going to prove more than Proposition 6.3. To this end, we prove

Lemma 6.4. *Let $S \in \mathbb{F}_{q^m} = k_0$. Then we have $\mu S \in \text{im } \wp$ for all $\mu \in \mathbb{F}_q$ if and only if there exists $\lambda \in \mathbb{F}_{q^m}$ such that $S = \lambda^q - \lambda$.*

Proof. We consider the homomorphism $g: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$, $g(\lambda) = \lambda^q - \lambda$. Then $\ker g = \mathbb{F}_q$ and $|\text{im } g| = \frac{q^m}{q}$. The Artin-Schreier homomorphism, $\wp: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$, $\wp(\lambda) = \lambda^p - \lambda$, satisfies $\ker \wp = \mathbb{F}_p$ and $|\text{im } \wp| = \frac{q^m}{p}$. Finally we consider $h: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ given by $h(\lambda) = \lambda + \lambda^p + \dots + \lambda^{p^{n-1}}$, $q = p^n$. Then $h(\lambda)^p - h(\lambda) = \lambda^q - \lambda$.

We have that

$$(\wp \circ h) = (h \circ \wp) = g.$$

Now, if $S = \lambda^q - \lambda$ for some $\lambda \in \mathbb{F}_{q^m}$, then $\mu S = (\mu\lambda)^q - (\mu\lambda)$ for all $\mu \in \mathbb{F}_q$ and we have

$$(\mu\lambda)^q - (\mu\lambda) = g(\mu\lambda) = \wp(h(\mu\lambda)) \in \text{im } \wp,$$

for all $\mu \in \mathbb{F}_q$.

Conversely, assume that $A := \{\mu S\}_{\mu \in \mathbb{F}_q} \subseteq \text{im } \wp$. If $S = 0$ there is nothing to prove. We consider $S \neq 0$. In case that $S \notin \text{im } g$ we would have $\mu S \notin \text{im } g$ for all $\mu \in \mathbb{F}_q^*$ since otherwise, if $\mu S = \lambda^q - \lambda$ for some $\lambda \in \mathbb{F}_{q^m}$ then for all $\mu \in \mathbb{F}_q$, $\mu^q = \mu$ and

$$S = \frac{\lambda^q}{\mu} - \frac{\lambda}{\mu} = \left(\frac{\lambda}{\mu}\right)^q - \left(\frac{\lambda}{\mu}\right) \in \text{im } g,$$

which is absurd.

Under this assumption the additive subgroup $A = \{\mu S\}_{\mu \in \mathbb{F}_q}$ of \mathbb{F}_{q^m} , which is of cardinality q , satisfies $A \cap \text{im } g = \{0\}$. Since $A \subseteq \text{im } \wp$ and because $g = \wp \circ h$, that is, $\text{im } g \subseteq \text{im } \wp$, it follows that $A + \text{im } g \subseteq \text{im } \wp$. But on the other hand

$$|A + \text{im } g| = |A| |\text{im } g| = q \cdot \frac{q^m}{q} = q^m > \frac{q^m}{p} = |\text{im } \wp|,$$

which is a contradiction. Thus $A \cap \text{im } g \neq \{0\}$. Therefore there exists $\mu \in \mathbb{F}_q^*$ with $\mu S \in \text{im } g$ which implies that $S \in \text{im } g$. This finishes the proof. \square

Let $f(X)$ be an additive polynomial given by (5.1). The result of Lemma 6.4 should hold in this case but we don't have a proof. Let $\mathcal{G}_f = \mathcal{L}_{\mathbb{F}_p}\{\varepsilon_1, \dots, \varepsilon_n\}$ and consider the following n subspaces of \mathcal{G}_f of codimension 1:

$$\mathcal{H}_i := \mathcal{L}_{\mathbb{F}_p}\{\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \varepsilon_n\}, \quad 1 \leq i \leq n.$$

Let $f_{\mathcal{H}_i}(X) = f_i(X)$, $a_i = f_i(\varepsilon_i) \neq 0$.

What we need is:

$$(6.2) \quad \bigcap_{i=1}^n \text{im } \wp_{a_i} = \text{im } f.$$

We have:

Proposition 6.5. *Let $K = k(y)/k$ with $f(y) = u$ and u given in a reduced form (5.3). We assume that \mathcal{P}_∞ is unramified in K/k . If $f(X) = X^q - X$ or if (6.2) holds, then \mathcal{P}_∞ decomposes fully if and only if $R(T) = 0$.*

Proof. First we consider the particular case $f(X) = X^q - X$. We have that \mathcal{P}_∞ decomposes fully in K/k if and only if it decomposes fully in every intermediate extension of degree p : $y_\mu^p - y_\mu = \mu u$ where $y_\mu = h(\mu y) = (\mu y)^{p^{n-1}} + \dots + (\mu y)^p + (\mu y)$, $\mu \in \mathbb{F}_q^*$. The latter is equivalent to $\mu R(T) \in \text{im } \wp(\mathbb{F}_{q^m})$ for all $\mu \in \mathbb{F}_q$. From Lemma 6.4 the latter is equivalent to $R(T) = \lambda^q - \lambda$ for some $\lambda \in \mathbb{F}_{q^m}$. Since u is in reduced form, it follows that $R(T) = 0$.

For the general case, from Theorem 5.5, \mathcal{P}_∞ decomposes fully in K/k if and only if \mathcal{P}_∞ decomposes in every subextension of degree p given by

$$(6.3) \quad z_{\mathcal{H}}^p - z_{\mathcal{H}} = \frac{u}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p},$$

for every hyperplane \mathcal{H} of \mathcal{G}_f . The term (6.3) that determines the behavior of \mathcal{P}_∞ is $\frac{R(T)}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p}$. Therefore \mathcal{P}_∞ decomposes fully in (6.3) if and only if $R(T) \in \text{im } \wp_{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})}$. Now the result is a consequence of equation (6.2). \square

Next, we present a result similar to that of Proposition 6.1 for a certain family of elementary abelian p -extensions. Note that when the infinite prime is ramified, we do not give the precise behavior of the prime in the extension.

Corollary 6.6. *Let $K = k_0(T)$ be a rational function field and $K = k(y)$ be an elementary abelian p -extension of k given by a reduced form*

$$y^q - y = u = \sum_{i=1}^r \frac{Q_i(T)}{P_i(T)^{\alpha_i}} + R(T)$$

satisfying the conditions of Theorem 5.3.

Then the prime divisor \mathcal{P}_∞ is

- (a).- *fully decomposed if $R(T) = 0$.*
- (b).- *not ramified with inertia degree p if $R(T) \in k_0$ and $R(T) \notin \{\lambda^q - \lambda \mid \lambda \in k_0\}$.*
- (c).- *ramified if $R(T) \notin k_0$.* □

Let $K = k(y)$ be given by (5.3) and let \mathcal{P}_i be the prime divisors associated to $P_i(T)$, $1 \leq i \leq r$. Let \mathcal{P} be a prime divisor such that $\mathcal{P} \notin \{\mathcal{P}_1, \dots, \mathcal{P}_r, \mathcal{P}_\infty\}$. Then \mathcal{P} is either fully decomposed in K/k or has inertia degree equal to p . The following results establish the decomposition type of \mathcal{P} .

First we study the Artin-Schreier case.

Proposition 6.7. *Let \mathcal{P} and K/k be as before. Let us write equation (6.1) as*

$$y^p - y = u(T),$$

with $u(T) = \frac{g(T)}{h(T)} \in k = k_0(T)$ such that $\gcd(g(T), h(T)) = 1$. Let $P(T) \in R_T^+$ be the irreducible polynomial associated to \mathcal{P} , say $\deg P(T) = m$. Let $\nu \in k'$ be a root of $P(T)$, where k' is the decomposition field of the polynomial $P(T)$. Then \mathcal{P} decomposes fully in K/k if and only if $u(\nu) \in \wp(k')$.

Proof. We have $[k' : k_0] = m$. Let $\nu = \nu_1, \dots, \nu_m$ be the roots of P in k' , $P(T) = \prod_{i=1}^m (T - \nu_i)$. We have that \mathcal{P} decomposes fully in $k'(T) := k_m/k = k_0(T)$. Here k_m denotes the constant extension of k of degree m . Since we are assuming that the extension K/k is geometric, it follows that $k_m \cap K = k$ and therefore \mathcal{P} decomposes fully in K/k if and only if \mathcal{Q} decomposes fully in K_m/k_m where $K_m = Kk_m$ and \mathcal{Q} is a prime in k_m above \mathcal{P} .

$$\begin{array}{ccc} K & \xrightarrow{\quad} & K_m \\ \downarrow & & \downarrow \\ k & \xrightarrow[\mathcal{P} \text{ decomposes fully}]{} & k_m \end{array}$$

Say that \mathcal{Q} is the prime divisor associated to $T - \nu \in k_m$. Since $v_{\mathcal{P}}(u(T)) \geq 0$ it follows that $v_{\mathcal{Q}}(u(T)) \geq 0$ so that $T - \nu \nmid h(T)$ and $h(\nu) \neq 0$. Furthermore $g(\nu) = 0 \iff v_{\mathcal{P}}(u(T)) > 0$. We have $\deg_{k_m} \mathcal{Q} = 1$. We make \mathcal{Q} the infinite prime in k_m , that is, let $T' = \frac{1}{T-\nu}$, $(T')_{k_m} = \frac{\mathcal{Q}_0'}{\mathcal{Q}'_\infty} = \frac{\mathcal{Q}_0}{\mathcal{Q}}$, where $(T)_{k_m} = \frac{\mathcal{Q}_0}{\mathcal{Q}_\infty}$. We have $T = \frac{1}{T'} + \nu$.

$$\text{Write } u_1(T') := u(T) = u\left(\frac{1}{T'} + \nu\right) = \frac{g\left(\frac{1}{T'} + \nu\right)}{h\left(\frac{1}{T'} + \nu\right)} = \frac{g\left(\frac{1}{T'}(1+T'\nu)\right)}{h\left(\frac{1}{T'}(1+T'\nu)\right)}.$$

Let $g(T) = a_s T^s + a_{s-1} T^{s-1} + \cdots + a_1 T + a_0$, $a_s \neq 0$, $a_i \in \mathbb{F}_q$, $0 \leq i \leq s$; $h(T) = b_t T^t + b_{t-1} T^{t-1} + \cdots + b_1 T + b_0$, $b_t \neq 0$, $b_j \in \mathbb{F}_q$, $0 \leq j \leq t$. Then

$$\begin{aligned} g\left(\frac{1}{T'}(1 + T'\nu)\right) &= \frac{1}{(T')^s} \left(a_s + \cdots + g(\nu)(T')^s\right) = \frac{1}{(T')^s} g_1(T'); \\ h\left(\frac{1}{T'}(1 + T'\nu)\right) &= \frac{1}{(T')^t} \left(b_t + \cdots + h(\nu)(T')^t\right) = \frac{1}{(T')^t} h_1(T'). \end{aligned}$$

It follows that

$$\deg_{T'} g_1(T') \leq s; \quad \deg_{T'} h_1(T') = t.$$

Therefore

$$\deg_{T'} u_1(T') = \deg_{T'} g_1(T') - s \leq 0, \quad \text{and} \quad v_{\mathcal{Q}}(u_1(T')) = s - \deg_{T'}(g_1(T')) \geq 0.$$

The reduced form of $u_1(T')$ is

$$u_1(T') = \sum_{j=1}^{r'} \frac{Q'_j(T')}{(P'_j(T'))^{e'_j}} + u(\nu).$$

Thus \mathcal{Q} decomposes fully in $K_m/k_m \iff u(\nu) \in \wp(k')$. This proves the proposition. \square

The general case is consequence of Proposition 6.7. Indeed, let $K = k(y)$ where y is given in a reduced form (5.3). We assume that \mathcal{P} is not ramified in K/k . From Theorem 5.5, using the notation given there, we have that every subextension of K of degree p over k is given by (6.3).

As a consequence of these expressions and from Propositions 6.5 and 6.7, we obtain the main result of this section.

Theorem 6.8. *With the above notations, let \mathcal{P} be a non-ramified in K/k prime divisor of degree m . Then we have that \mathcal{P} decomposes fully in $K/k \iff$ for every hyperplane \mathcal{H} holds*

$$u(\nu) \frac{1}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p} \in \wp(k'),$$

and \mathcal{P} has inertia degree p in $K/k \iff$ there exists an hyperplane \mathcal{H} such that

$$u(\nu) \frac{1}{f_{\mathcal{H}}(\varepsilon_{\mathcal{H}})^p} \notin \wp(k').$$

Equivalently, if (6.2) holds, then \mathcal{P} decomposes fully in $K/k \iff u(\nu) \in f(k')$. \square

7. GENERATORS OF ELEMENTARY ABELIAN p -EXTENSIONS

Let k be an arbitrary field of characteristic $p > 0$ and let $f(X) \in k[X]$ be an additive polynomial given by (5.1) such that $\mathcal{G}_f \subseteq k$. Let $u \in k$ be such that $F(X) = f(X) - u \in k[X]$ is irreducible. Let $K = k(y)$ where $f(y) = u$, $\text{Gal}(K/k) \cong \mathcal{G}_f$. We have that K/k has $\frac{(p^n-1)(p^n-p)\cdots(p^n-p^{m-1})}{(p^m-1)(p^m-p)\cdots(p^m-p^{m-1})}$ subextensions $k \subseteq E \subseteq K$ such that $[E : k] = p^m$.

We want to study the relation between y and z in case $K = k(y) = k(z)$ and $f(z) = \chi \in k$. The next result is well known.

Proposition 7.1. *If $k(y_1)$ y $k(y_2)$ are cyclic extensions of degree p of k with $\wp(y_i) = x_i \in k$, $i = 1, 2$, the following two statements are equivalent:*

- (a).- $k(y_1) = k(y_2)$,
- (b).- *there exist $j \in \mathbb{F}_p^*$ and $z \in k$ such that $y_1 = jy_2 + z$ and $x_1 = jx_2 + \wp(z)$.* \square

Next theorem generalizes Propostition 7.1. This is the main result of this section.

Theorem 7.2. *With the above notation we have that the following statements are equivalent:*

- (a).- $k(y) = k(z)$,
- (b).- *there exist $A_{n-1}, A_{n-2}, \dots, A_1, A_0 \in \mathcal{G}_f$ satisfying*

$$A_{n-1}\beta^{p^{n-1}} + A_{n-2}\beta^{p^{n-2}} + \dots + A_2\beta^{p^2} + A_1\beta^p + A_0\beta = 0$$

with $\beta \in \mathcal{G}_f \iff \beta = 0$

and $D \in k$ such that

$$(7.1) \quad z = A_{n-1}y^{p^{n-1}} + A_{n-2}y^{p^{n-2}} + \dots + A_2y^{p^2} + A_1y^p + A_0y + D.$$

Theorem 7.2 is an immediate consequence of the following more general theorem.

Theorem 7.3. *Let $K = k(y)$. Then the following statements are equivalent:*

- (a).- *$E = k(z)$ with $k \subseteq E \subseteq K$, $[E : k] = p^m$ such that $g(z) = \chi \in k$ for some $\chi \in k$ and for some additive polynomial $g(X)$ such that $g(X) \mid f(X)$, that is, $g = f_V$ for an additive subgroup V of \mathcal{G}_f of dimension m over \mathbb{F}_p ,*
- (b).- *there exist $A_{n-1}, A_{n-2}, \dots, A_1, A_0 \in \mathcal{G}_f$, $C \in k$ and a \mathbb{F}_p -vector subspace \mathcal{H} of \mathcal{G}_f of dimension $n - m$ such that*

$$(7.2) \quad z = A_{n-1}y^{p^{n-1}} + A_{n-2}y^{p^{n-2}} + \dots + A_2y^{p^2} + A_1y^p + A_0y + C,$$

- (2) *for $\beta \in \mathcal{G}_f$,*

$$A_{n-1}\beta^{p^{n-1}} + A_{n-2}\beta^{p^{n-2}} + \dots + A_2\beta^{p^2} + A_1\beta^p + A_0\beta = 0 \iff \beta \in \mathcal{H}.$$

The relation between E and (7.2) is given as follows. If $\mathcal{H} = \mathcal{L}_{\mathbb{F}_p}\{\mu_{m+1}, \dots, \mu_n\}$ where $\{\mu_1, \dots, \mu_n\}$ is the basis of \mathcal{G}_f such that if $G = \langle \sigma_1, \dots, \sigma_n \rangle$, $\sigma_i(y) = y + \mu_i$, $1 \leq i \leq n$, then E is the fixed field by the subgroup $H := \langle \sigma_{m+1}, \dots, \sigma_n \rangle$ of G . That is, H corresponds to \mathcal{H} under the isomorphism given in Proposition 2.2 and if $\mathcal{G}_f = \mathcal{H} \oplus V$, $g(X) = f_V(X) = \prod_{\delta \in V} (X - \delta) \mid f(X)$.

Proof. Let $G = \text{Gal}(K/k) = \langle \sigma_1, \dots, \sigma_n \rangle$ with $\sigma_i(y) = y + \mu_i$, where $\mu_i \in \mathcal{G}_f$ and $\{\mu_1, \dots, \mu_n\}$ is a \mathbb{F}_p -basis of \mathcal{G}_f . More precisely, we have that if $\sigma_1, \dots, \sigma_n \in G$ with $\sigma_i(y) = y + \mu_i$, then $G = \langle \sigma_1, \dots, \sigma_n \rangle \iff \{\mu_1, \dots, \mu_n\}$ is a basis of $\mathcal{G}_f/\mathbb{F}_p$. Note that for $0 \leq \alpha_i \leq p-1$, $1 \leq i \leq n$, $\sigma = \sigma_1^{\alpha_1} \dots \sigma_n^{\alpha_n}$ we have $\sigma(y) = y + \sum_{i=1}^n \alpha_i \mu_i$.

First we consider a subfield E of K of degree p^m over k . We may choose a set of n generators of $G = \text{Gal}(K/k) = \langle \sigma_1, \dots, \sigma_n \rangle$ in such a way that $E = K^{\langle \sigma_{m+1}, \dots, \sigma_n \rangle}$ is the fixed field under $H = \langle \sigma_{m+1}, \dots, \sigma_n \rangle$. We have $\text{Gal}(K/E) = \langle \sigma_{m+1}, \dots, \sigma_n \rangle$.

Let $\theta: G \rightarrow \mathcal{G}_f$ be the isomorphism given by $\sigma_i \mapsto \mu_i$, $1 \leq i \leq n$. Let $\mathcal{H} = \theta(H) < \mathcal{G}_f$ and let V be an arbitrary section of the exact sequence

$$0 \longrightarrow \mathcal{H} \xrightarrow{i} \mathcal{G}_f \xrightarrow{\pi} \mathcal{G}_f/\mathcal{H} \longrightarrow 0,$$

that is, $V = \varphi(\mathcal{G}_f/\mathcal{H}) < \mathcal{G}_f$ where $\varphi: \mathcal{G}_f/\mathcal{H} \longrightarrow \mathcal{G}_f$ satisfies $\pi \circ \varphi = \text{Id}_{\mathcal{G}_f/\mathcal{H}}$. We have $\mathcal{G}_f \cong \mathcal{H} \oplus V$ as \mathbb{F}_p -vector spaces.

From Theorem 5.7, we have that there exist $z \in E$ and $\chi \in k$ such that $E = k(z)$ with $f_V(z) = \chi \in k$ and $f_V(X) = \prod_{\delta \in V} (X - \delta) \mid \prod_{\delta \in \mathcal{G}_f} (X - \delta) = f(X)$.

We have that $\text{Gal}(E/k) \cong \langle \bar{\sigma}_1, \dots, \bar{\sigma}_m \rangle$ where $\bar{\sigma}_i = \sigma_i|_E$ or, equivalently, $\bar{\sigma}_i = \sigma_i \bmod \text{Gal}(K/E)$.

Now, let $\sigma_i(z) = z + \gamma_i$, $1 \leq i \leq m$, where $\{\gamma_1, \dots, \gamma_m\}$ is a basis of V and $\sigma_j(z) = z$ for $m+1 \leq j \leq n$. We denote $\gamma_j = 0$ for $m+1 \leq j \leq n$.

Let $A_{n-1}, A_{n-2}, \dots, A_1, A_0 \in \mathcal{G}_f$ be arbitrary and let

$$(7.3) \quad w := A_{n-1}y^{p^{n-1}} + A_{n-2}y^{p^{n-2}} + \dots + A_2y^{p^2} + A_1y^p + A_0y.$$

That is, if we denote $l(X) = A_{n-1}X^{p^{n-1}} + \dots + A_1X^p + A_0X$, then $w = l(y)$.

We will prove that there exist $A_{n-1}, A_{n-2}, \dots, A_1, A_0 \in \mathcal{G}_f$ and $D \in k$ such that

$$(7.4) \quad z = w + D.$$

We have

$$(7.5) \quad \sigma_i(w) = \sigma_i(l(y)) = l(\sigma_i(y)) = l(y + \mu_i) = l(y) + l(\mu_i) = w + l(\mu_i).$$

It follows that

$$(7.6) \quad \sigma_i(w) = w + \gamma_i, \quad 1 \leq i \leq n \iff l(\mu_i) = \gamma_i, \quad 1 \leq i \leq n$$

$$\iff M \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{n-2} \\ A_{n-1} \end{bmatrix} = \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_{n-1} \\ \gamma_n \end{bmatrix} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_m \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

where M is the matrix

$$M = \begin{bmatrix} \mu_1 & \mu_1^p & \cdots & \mu_1^{p^{n-2}} & \mu_1^{p^{n-1}} \\ \mu_2 & \mu_2^p & \cdots & \mu_2^{p^{n-2}} & \mu_2^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n-1} & \mu_{n-1}^p & \cdots & \mu_{n-1}^{p^{n-2}} & \mu_{n-1}^{p^{n-1}} \\ \mu_n & \mu_n^p & \cdots & \mu_n^{p^{n-2}} & \mu_n^{p^{n-1}} \end{bmatrix}.$$

We will prove that M is non-singular. Let

$$B(X) := \begin{bmatrix} X & X^p & \cdots & X^{p^{n-2}} & X^{p^{n-1}} \\ \mu_2 & \mu_2^p & \cdots & \mu_2^{p^{n-2}} & \mu_2^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n-1} & \mu_{n-1}^p & \cdots & \mu_{n-1}^{p^{n-2}} & \mu_{n-1}^{p^{n-1}} \\ \mu_n & \mu_n^p & \cdots & \mu_n^{p^{n-2}} & \mu_n^{p^{n-1}} \end{bmatrix} = \begin{bmatrix} F(X) \\ F(\mu_2) \\ \vdots \\ F(\mu_{n-1}) \\ F(\mu_n) \end{bmatrix}$$

where $F(Z) := [Z \quad Z^p \quad \cdots \quad Z^{p^{n-2}} \quad Z^{p^{n-1}}]$ with $Z \in \{X, \mu_2, \dots, \mu_n\}$ denotes the rows of $B(X)$. We have $B(\mu_1) = M$ and $\det B(X)$ is an additive polynomial in $k[X]$ of degree p^{n-1} .

Let $\{i_2, \dots, i_n\} \subseteq \mathbb{F}_p^{n-1}$ and $\xi = i_2\mu_2 + \dots + i_n\mu_n$. Then:

$$B(\xi) = \begin{bmatrix} F(i_2\mu_2 + \dots + i_n\mu_n) \\ F(\mu_2) \\ \vdots \\ F(\mu_{n-1}) \\ F(\mu_n) \end{bmatrix} = \begin{bmatrix} i_2F(\mu_2) + \dots + i_nF(\mu_n) \\ F(\mu_2) \\ \vdots \\ F(\mu_{n-1}) \\ F(\mu_n) \end{bmatrix}.$$

Therefore $\det B(\xi) = 0$ for every $\xi \in \{i_2\mu_2 + \dots + i_n\mu_n \mid i_2, \dots, i_n \in \mathbb{F}_p\} = C$. Since $\{\mu_2, \dots, \mu_n\}$ is a linearly independent set over \mathbb{F}_p , it follows that $|C| = p^{n-1} = \deg B(X)$. In this way, we obtain that C is the set of roots of $\det B(X)$. In particular, since $\mu_1 \notin C$, $\det B(\mu_1) = \det M \neq 0$ and M is non-singular.

Hence (7.6) has a unique solution:

$$(7.7) \quad \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{n-2} \\ A_{n-1} \end{bmatrix} = M^{-1} \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_m \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let $\beta = \sum_{i=1}^n c_i\mu_i \in \mathcal{G}_f$ with $c_i \in \mathbb{F}_p$, $1 \leq i \leq n$. Therefore

$$l(\beta) = l\left(\sum_{i=1}^n c_i\mu_i\right) = \sum_{i=1}^n l(c_i\mu_i) = \sum_{i=1}^n c_i l(\mu_i) = \sum_{i=1}^n c_i \gamma_i = \sum_{i=1}^m c_i \gamma_i.$$

It follows that $l(\beta) = 0 \iff c_1 = \dots = c_m = 0 \iff \beta \in \mathcal{L}_{\mathbb{F}_p}\{\mu_{m+1}, \dots, \mu_n\} = \mathcal{H}$.

Finally, we have $\sigma_i(z - w) = z - w$ for all $1 \leq i \leq n$, so that $z - w = D \in k$ and z is in the form (7.2).

To prove the converse, let z be given by (7.2), $z = l(y) + D$. Then

$$\sigma_i(z) = \sigma_i(l(y) + D) = l(\sigma_i(y)) + D = l(y + \mu_i) + D = l(y) + l(\mu_i) + D = z + l(\mu_i)$$

and we have $l(\mu_i) = 0 \iff i \geq m + 1$. Therefore $k(z) \subseteq K^{(\sigma_{m+1}, \dots, \sigma_n)}$. Now, for any $c_1, \dots, c_m \in \mathbb{F}_p$, not all equal to zero, $\sigma_1^{c_1} \dots \sigma_m^{c_m}(z) = z + l(\beta)$ with $\beta = \sum_{i=1}^m c_i\mu_i \neq 0$, $l(\beta) \neq 0$. This implies that $[k(z) : k] \geq p^m$. It follows that $[k(z) : k] = p^m$ and that $k(z) = K^{(\sigma_{m+1}, \dots, \sigma_n)}$.

Let $\xi_i := l(\mu_i)$, $1 \leq i \leq m$, $V = \mathcal{L}_{\mathbb{F}_p}\{\xi_1, \dots, \xi_m\}$ and $f_V(X) \mid f(X)$. Then

$$f_V(z) = f_V(l(y) + D) = f_V\left(\sum_{i=0}^{n-1} A_i y^{p^i} + D\right) = \sum_{i=0}^{n-1} f_V(A_i y^{p^i}) + f_V(D) = \chi.$$

We will prove that $\chi = f_V(z) \in k$.

If $\sigma := \sigma_1^{c_1} \dots \sigma_n^{c_n} \in G = \text{Gal}(K/k)$ then, for $\mu := \sum_{i=1}^n c_i\mu_i$, $\sigma(y) = y + \mu$, we have

$$\begin{aligned} \sigma(f_V(z)) &= \sigma(f_V(l(y) + D)) = f_V(l(y + \mu) + D) = f_V(l(y) + l(\mu) + D) \\ &= f_V(l(y) + D) + f_V(l(\mu)) = f_V(z) + f_V(l(\mu)). \end{aligned}$$

Finally,

$$l(\mu) = \sum_{i=1}^n c_i l(\mu_i) = \sum_{i=1}^m c_i \gamma_i \in V,$$

so that $f_V(l(\mu)) = 0$ and $\sigma(f_V(z)) = f_V(z)$ for all $\sigma \in \text{Gal}(K/k)$. It follows that $\chi = f_V(z) \in k$. This finishes the proof. \square

8. MULTICYCLIC EXTENSIONS

In this section we are interested in abelian extensions with Galois group isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^n$. To this end, we generalize the results of previous sections and consider extensions using the Witt ring. First we fix some notation that will be used in this part of the paper. For details, the main sources are the papers of Witt [8] and of Schmid [6]. A summary can be found in [4, Capítulo 11].

Given a commutative ring with identity R , $W_m(R)$ denotes the ring of Witt vectors over R of length m , that is, $\vec{\alpha} = (\alpha_1, \dots, \alpha_m \mid \alpha^{(1)}, \dots, \alpha^{(m)}) \in W_m(R)$ means that $\alpha_i \in R$, $1 \leq i \leq m$ and that $\alpha^{(i)} = \alpha_1^{p^{i-1}} + p\alpha_2^{p^{i-2}} + \dots + p^{i-1}\alpha_i$ are the ghost components of $\vec{\alpha}$. Witt operations are denoted by $\dot{+}, \dot{-}, \dot{\cdot}$. Let $\vec{1} = (1, 0, \dots, 0)$ and for $t \in \mathbb{N}$, $\vec{t} = \underbrace{\vec{1} \dot{+} \dots \dot{+} \vec{1}}_{t \text{ times}}$. We have $\vec{p}^j \dot{\cdot} \vec{1} = (\underbrace{0, 0, \dots, 0}_j, \overset{\uparrow}{1}_{j+1}, 0, \dots, 0)$. Furthermore

$$W_m(\mathbb{F}_p) \cong \mathbb{Z}/p^m\mathbb{Z}.$$

For $u \in R$ we write $\{u\} := (u, 0, \dots, 0 \mid u, u^p, \dots, u^{p^{m-1}})$. For a vector $\vec{x} = (x_1, \dots, x_m) \in W_m(R)$, we define $\vec{x}^p := (x_1^p, \dots, x_m^p)$. Note that \vec{x}^p is not the p -power of \vec{x} with Witt multiplication, that is, $\vec{x}^p \neq \underbrace{\vec{x} \dot{\cdot} \dots \dot{\cdot} \vec{x}}_p$. The Artin-Schreier-

Witt operator is defined by $\wp(\vec{x}) := \vec{x}^p \dot{-} \vec{x}$.

Let k be a field of characteristic p . Then $\wp(\vec{x}) = \vec{0} \iff \vec{x} \in W_m(\mathbb{F}_p) \subseteq W_m(k)$. We have $(\vec{x} \dot{\cdot} \vec{y})^p = \vec{x}^p \dot{\cdot} \vec{y}^p$ where $\circ \in \{+, -, \cdot\}$. Let K/k be a cyclic extension of degree p^m . Here we write, for $\vec{y} = (y_1, \dots, y_m)$, $\sigma\vec{y} = (\sigma y_1, \dots, \sigma y_m)$. Let $G = \text{Gal}(K/k) = \langle \sigma \rangle$, $\sigma(\sigma) = p^m$. Now $\vec{1} \in W_m(K)$ satisfies

$$\text{Tr}_{K/k} \vec{1} = \sum_{\sigma \in G} \sigma \vec{1} = \vec{p}^m \dot{\cdot} \vec{1} = \vec{p}^m = \vec{0}.$$

Thus there exists $\vec{y} \in W_m(K)$ such that $(\sigma \dot{-} \vec{1})(\vec{y}) = \vec{1}$, that is, $\sigma\vec{y} = \vec{y} \dot{+} \vec{1}$.

Let $\vec{x} := \wp\vec{y} = \vec{y}^p \dot{-} \vec{y}$. Then

$$\sigma(\wp\vec{y}) = \wp(\sigma\vec{y}) = \wp(\vec{y} \dot{+} \vec{1}) = \wp(\vec{y}) \dot{+} \wp(\vec{1}) = \wp(\vec{y}),$$

so, we obtain that $\vec{x} \in W_m(k)$. Now, $\sigma(\vec{y}) = \vec{y} \dot{+} \vec{1}$ where $k(\vec{y}) := k(y_1, \dots, y_m) \subseteq K$ and $k(\vec{y})/k$ is a cyclic extension of degree p^m because $\sigma^t\vec{y} = \vec{y} \dot{+} \vec{t}$ and p^m is minimum satisfying $\vec{p}^m = \vec{0}$. Therefore $K = k(\vec{y})$.

In general, if k is a field of characteristic p , the vector $\vec{y} \in W_m(k)$ is invertible $\iff y_1 \neq 0$.

The following Proposition generalizes Proposition 7.1.

Proposition 8.1. *If $k(\vec{y}_1)$ and $k(\vec{y}_2)$ are cyclic extensions of degree p^m of k with $\vec{y}_1, \vec{y}_2 \in W_m(K)$ and $\wp(\vec{y}_i) = \vec{x}_i \in W_m(k)$, $i = 1, 2$, then the following statements are equivalent:*

- (a).- $k(\vec{y}_1) = k(\vec{y}_2)$,
 (b).- there exist $\vec{j} \in W_m(\mathbb{F}_p)$ invertible, that is, $\gcd(j, p) = 1$, and $\vec{z} \in W_m(k)$ such that $\vec{y}_1 = \vec{j} \cdot \vec{y}_2 \dot{+} \vec{z}$ and $\vec{x}_1 = \vec{j} \cdot \vec{x}_2 \dot{+} \wp(\vec{z})$. \square

Let $q = p^n$ and consider a field k such that $\mathbb{F}_q \subseteq k$. Let $\vec{x}^q := (x_1^q, \dots, x_m^q)$. Then $\vec{x}^q \dot{-} \vec{x} = 0 \iff \vec{x} \in W_m(\mathbb{F}_q) \subseteq W_m(k)$. The ring $W_m(\mathbb{F}_q)$ is known as a *Galois ring*. As group, we see that $W_m(\mathbb{F}_q)$ is a free $W_m(\mathbb{F}_p)$ -module of rank n . In particular, $W_m(\mathbb{F}_q) \cong (\mathbb{Z}/p^m\mathbb{Z})^n$ as groups.

Proposition 8.2. *We have that $W_m(\mathbb{F}_q)$ is a free $W_m(\mathbb{F}_p)$ -module of rank n , where $q = p^n$. More precisely, let $\{\mu_1, \dots, \mu_n\}$ be a basis of \mathbb{F}_q over \mathbb{F}_p and set $\vec{\mu}_i := \{\mu_i\} = (\mu_i, 0, \dots, 0)$, $1 \leq i \leq n$. Then $\{\vec{\mu}_1, \dots, \vec{\mu}_n\}$ is a $W_m(\mathbb{F}_p)$ -basis of $W_m(\mathbb{F}_q)$. That is*

$$W_m(\mathbb{F}_q) = \bigoplus_{i=1}^n W_m(\mathbb{F}_p) \cdot \vec{\mu}_i.$$

Proof. Let $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in W_m(\mathbb{F}_p)$, with $\vec{\alpha}_i = (\alpha_{i1}, \dots, \alpha_{im} \mid \alpha_i^{(1)}, \dots, \alpha_i^{(m)})$, $\vec{\mu}_i = (\mu_i, 0, \dots, 0 \mid \mu_i, \mu_i^p, \dots, \mu_i^{p^{m-1}})$. We have that $\vec{\alpha}_i \cdot \vec{\mu}_i = (\alpha_{i1}\mu_i, \dots, ? \mid \alpha_{i1}\mu_i, \dots, ?)$. If $\sum_{i=1}^n \vec{\alpha}_i \vec{\mu}_i = (\dots \mid \sum_{i=1}^n \alpha_{i1}\mu_i, \dots) = \vec{0} = (0, \dots, 0 \mid 0, \dots, 0)$, we obtain that $\sum_{i=1}^n \alpha_{i1}\mu_i = 0$ which implies $\alpha_{i1} = 0$ for all $1 \leq i \leq n$.

We obtain $\vec{\alpha}_i = (0, \alpha_{i2}, \dots, \alpha_{im} \mid 0, p\alpha_{i2}, \dots)$. Therefore, the second ghost component of $\sum_{i=1}^n \vec{\alpha}_i \cdot \vec{\mu}_i = \vec{0}$ is $\vec{0}^{(2)} = \sum_{i=1}^n p\alpha_{i2}\mu_i^p$. Thus

$$0 = \vec{0}_2 = \frac{1}{p}(\vec{0}^{(2)} - \vec{0}_1^p) = \sum_{i=1}^n \alpha_{i2}\mu_i^p = \sum_{i=1}^n \alpha_{i2}^p \mu_i^p = \left(\sum_{i=1}^n \alpha_{i2}\mu_i \right)^p = 0.$$

Hence $\sum_{i=1}^n \alpha_{i2}\mu_i = 0$ so that $\alpha_{i2} = 0$ for all $1 \leq i \leq n$. Keeping on with this procedure, we obtain $\vec{\alpha}_i = \vec{0}$ and the result follows. \square

Remark 8.3. In general we have that $\{\vec{\xi}_1, \dots, \vec{\xi}_n\}$ is a basis of $W_m(\mathbb{F}_q)$ over $W_m(\mathbb{F}_p)$ if and only if $\{\xi_{11}, \dots, \xi_{n1}\}$ is a basis of \mathbb{F}_q sobre \mathbb{F}_p . This can be proved following the proof of Proposition 8.2 and noting that if $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in W_m(\mathbb{F}_p)$, then $\sum_{i=1}^n \vec{\alpha}_i \cdot \vec{\xi}_i = (\sum_{i=1}^n \alpha_{i1}\xi_{i1}, \dots)$, etc. We leave the details of the proof to the interested reader.

We consider the equation $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha}$ where $\vec{\alpha} \in W_m(k)$. Let $\vec{y}_0 \in W_m(\bar{k})$ be a solution of $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha}$, where \bar{k} denotes an algebraic closure of k . Note that if $K = k(\vec{y}) = k(y_1, \dots, y_m)$ is a cyclic extension of degree p^m over k , then $y_m \notin k(y_1, \dots, y_{m-1})$ since otherwise we would have that $[K : k] = [k(y_1, \dots, y_{m-1}) : k] \leq p^{m-1}$. So, $K = k(y_m)$. The set of roots of $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha}$ is the set $\{\vec{y}_0 \dot{+} \vec{\mu} \mid \vec{\mu} \in W_m(\mathbb{F}_q)\}$. Let $K = k(\vec{y}_0)$. Then, because $\mathbb{F}_q \subseteq k$, we have $W_m(\mathbb{F}_q) \subseteq W_m(k)$ and therefore K/k is a normal extension. Since $|W_m(\mathbb{F}_q)| = q^m = p^{nm}$, all the roots of $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha}$ are different and therefore K/k is a Galois extension.

Let $G := \text{Gal}(K/k)$ and $\sigma \in G$. Then \vec{y}_0 and $\sigma(\vec{y}_0)$ are conjugate so there exists $\vec{\xi} \in W_m(\mathbb{F}_q)$ such that $\sigma(\vec{y}_0) = \vec{y}_0 \dot{+} \vec{\xi}$. Put $\sigma_{\vec{\xi}} = \sigma$.

Proposition 8.4. *With the above notation, we have that $\varphi: G \rightarrow W_m(\mathbb{F}_q)$, given by $\varphi(\sigma_\xi) = \xi$ is a group monomorphism. This implies that the extension K/k is abelian and that $G \subseteq W_m(\mathbb{F}_q) \cong (\mathbb{Z}/p^m\mathbb{Z})^n$. Therefore $G \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n}\mathbb{Z}$ with $m \geq a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$. \square*

Conversely, let $K = k(z)$ be a finite abelian p -extension of exponent m and rank n , that is $G \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n}\mathbb{Z}$ with $m \geq a_1 \geq a_2 \geq \cdots \geq a_n \geq 1$ and we assume that $\mathbb{F}_q \subseteq k$ where $q = p^n$. Let $K = k(z_1, \dots, z_n)$ with $\text{Gal}(k(z_i)/k) \cong \mathbb{Z}/p^{a_i}\mathbb{Z}$, $1 \leq i \leq n$. Then, there exists \vec{y}_i such that $k(z_i) = k(\vec{y}_i)$ with $\vec{y}_i^p \dot{-} \vec{y}_i = \vec{\alpha}_i \in W_m(k)$, $\vec{y}_i \in W_m(K)$, where we write $\vec{y}_i = (\underbrace{0, \dots, 0}_{m-a_i}, y_{i,m-a_i+1}, \dots, y_{i,m})$, that is,

we complete with zeros the components to make the vectors of length m .

Let $G = \langle \sigma_1, \dots, \sigma_n \rangle$ with $\sigma_j(\vec{y}_i) = \begin{cases} \vec{y}_i \dot{+} \vec{1} & \text{if } i = j \\ \vec{y}_i & \text{if } i \neq j \end{cases}$, and $o(\sigma_i) = p^{a_i}$. We define

$$\vec{y} := \vec{\xi}_1 \dot{+} \vec{y}_1 \dot{+} \cdots \dot{+} \vec{\xi}_n \dot{+} \vec{y}_n,$$

where $\{\vec{\xi}_1, \dots, \vec{\xi}_n\}$ is a basis of $W_m(\mathbb{F}_q)$ over $W_m(\mathbb{F}_p)$. Then $\vec{y}_i \in W_m(K)$, $\vec{\xi}_i \in W_m(\mathbb{F}_q) \subseteq W_m(K)$. It follows that $k(\vec{y}) \subseteq K$. We will show that $k(\vec{y}) = K$.

Let $\sigma \in G$, say $\sigma = \sigma_1^{b_1} \cdots \sigma_n^{b_n}$, $0 \leq b_i \leq a_i - 1$, $1 \leq i \leq n$. Then, writing $\vec{b}_i = \{b_i\}$,

$$\begin{aligned} \sigma \vec{y} &= \sigma \left(\sum_{i=1}^n (\vec{\xi}_i \dot{+} \vec{y}_i) \right) = \sum_{i=1}^n \sigma(\vec{\xi}_i \dot{+} \vec{y}_i) \\ &= \sum_{i=1}^n \vec{\xi}_i \dot{+} \sigma(\vec{y}_i) = \sum_{i=1}^n \vec{\xi}_i \dot{+} (\vec{y}_i \dot{+} \vec{b}_i) \\ &\quad \uparrow \\ &\quad \vec{\xi}_i \in W_m(\mathbb{F}_q) \\ &= \sum_{i=1}^n \vec{\xi}_i \dot{+} \vec{y}_i \dot{+} \sum_{i=1}^n \vec{b}_i \dot{+} \vec{\xi}_i = \vec{y} \dot{+} \vec{\xi}, \end{aligned}$$

where $\vec{\xi} := \sum_{i=1}^n \vec{b}_i \dot{+} \vec{\xi}_i \in W_m(\mathbb{F}_q)$. Therefore $\sigma \vec{y} = \vec{y} \iff \vec{\xi} = \vec{0} \iff \vec{b}_1 = \cdots = \vec{b}_n = \vec{0} \iff b_1 = \cdots = b_n = 0 \iff \sigma = \text{Id}$. It follows that $K = k(\vec{y})$.

In brief, we have:

Theorem 8.5. *Let k be a field of characteristic $p > 0$ such that $\mathbb{F}_q \subseteq k$ with $q = p^n$. Let $\vec{\alpha} \in W_m(k)$. If $K = k(\vec{y}_0)$ where \vec{y}_0 is a root of $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha} \in W_m(k)$, then K/k is an abelian p -extension of exponent p^h with $h \leq m$ and rank l with $l \leq n$. Furthermore, if $G := \text{Gal}(K/k)$, we have that G is isomorphic in a natural way to a subgroup of the Galois ring $W_m(\mathbb{F}_q)$.*

Conversely, if $K = k(\vec{y}_0)$ is an abelian p -extension of exponent p^h and rank l , then \vec{y}_0 is root of some equation of the form $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha}$ for some $\vec{\alpha} \in W_m(k)$. \square

Now consider a finite abelian p -extension K/k given by $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha} \in W_m(k)$ and where we assume that $\mathbb{F}_q \subseteq k$. Say that $G = \text{Gal}(K/k) \cong \prod_{i=1}^n \mathbb{Z}/p^{a_i}\mathbb{Z}$ with $m \geq a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$. Let $\vec{\xi} \in W_m(\mathbb{F}_q)$ and let

$$(8.1) \quad \vec{y}_{\vec{\xi}} := (\vec{\xi}^{p^{n-1}} \dot{+} \vec{y}^{p^{n-1}}) \dot{+} (\vec{\xi}^{p^{n-2}} \dot{+} \vec{y}^{p^{n-2}}) \dot{+} \cdots \dot{+} (\vec{\xi}^p \dot{+} \vec{y}^p) \dot{+} (\vec{\xi} \dot{+} \vec{y}).$$

Then

$$\vec{y}_{\vec{\xi}}^p \dot{-} \vec{y}_{\vec{\xi}} = \vec{\xi} \dot{\cdot} \vec{\alpha},$$

that is, $k(\vec{y}_{\vec{\xi}})/k$ is a cyclic extension of degree p^h with $h \leq m$.

From now on, we will assume that $G := \text{Gal}(K/k) = \langle \sigma_1, \dots, \sigma_n \rangle \cong (\mathbb{Z}/p^m\mathbb{Z})^n$ with $o(\sigma_i) = p^m$ for all $1 \leq i \leq n$. The group G has $\frac{p^m - p^{m-1}}{p^m - p^{m-1}}$ distinct cyclic subgroups of order p^m . In particular, we must have $\alpha_1 \neq 0$. We want to verify that among all the extensions $k(\vec{y}_{\vec{\xi}})$ are all the cyclic subextensions of degree p^m . Under the isomorphism $G \cong W_m(\mathbb{F}_q)$, we consider $\sigma_i := \sigma_{\vec{\xi}_i}$, $1 \leq i \leq n$ where $\{\xi_1, \dots, \xi_n\}$ is a basis of \mathbb{F}_q sobre \mathbb{F}_p and where we recall that $\vec{\xi}_i = \{\xi_i\} = (\xi_i, 0, \dots, 0)$. In fact we note that $\{\xi_1, \dots, \xi_n\}$ is a basis \mathbb{F}_q over \mathbb{F}_p if and only if $G = \langle \sigma_1, \dots, \sigma_n \rangle$.

It is easy to see that for $\sigma_{\vec{\delta}} \in G$ we have $\sigma_{\vec{\delta}}(\vec{y}_{\vec{\xi}}) = \vec{y}_{\vec{\xi}} \dot{+} \sum_{i=0}^{n-1} (\vec{\xi} \dot{\cdot} \vec{\delta})^{p^i}$. Then $\sigma_{\vec{\delta}}(\vec{y}_{\vec{\xi}}) = \vec{y}_{\vec{\xi}} \iff \sum_{i=0}^{n-1} (\vec{\xi} \dot{\cdot} \vec{\delta})^{p^i} = \vec{0}$.

In general, let $g_{\vec{\xi}}(\vec{\delta}) := \sum_{i=0}^{n-1} (\vec{\xi} \dot{\cdot} \vec{\delta})^{p^i}$. Then $g_{\vec{\xi}}(\vec{\delta})^p \dot{-} g_{\vec{\xi}}(\vec{\delta}) = \vec{0}$, that is, $g_{\vec{\xi}}(\vec{\delta}) \in W_m(\mathbb{F}_p)$. The map $g_{\vec{\xi}}: W_m(\mathbb{F}_q) \rightarrow W_m(\mathbb{F}_p)$ is not surjective in general and we have

$$\frac{W_m(\mathbb{F}_q)}{\ker g_{\vec{\xi}}} \cong \text{im } g_{\vec{\xi}} \subseteq W_m(\mathbb{F}_p), \quad |W_m(\mathbb{F}_p)| = p^m,$$

so that $|\ker g_{\vec{\xi}}| \geq \frac{|W_m(\mathbb{F}_q)|}{|W_m(\mathbb{F}_p)|} = \frac{q^m}{p^m}$.

Observe $k(\vec{y}_{\vec{\xi}})$ is the fixed field of K by $\ker g_{\vec{\xi}}$.

Proposition 8.6. *With the notation as above and $\vec{\xi} = (\xi_1, \dots, \xi_m)$, we have that $[k(\vec{y}_{\vec{\xi}}) : k] = p^m \iff \vec{\xi}$ is invertible in $W_m(\mathbb{F}_q) \iff \xi_1 \neq 0$.*

Proof. In the expression $\sum_{i=0}^{n-1} (\vec{\xi} \dot{\cdot} \vec{\delta})^{p^i}$, the first component is $\sum_{i=0}^{n-1} (\xi_1 \delta_1)^{p^i}$. Assume that $\vec{\xi}$ is invertible, that is, $\xi_1 \neq 0$. Consider the map $\psi: \mathbb{F}_q \rightarrow \mathbb{F}_p$ given by $\psi(\delta) = \sum_{i=0}^{n-1} (\xi_1 \delta)^{p^i}$. This map is not zero since the polynomial $p(x) = (\xi_1 x)^{p^{n-1}} + \dots + (\xi_1 x)^p + (\xi_1 x) = 0$ has p^{n-1} roots. Therefore, if we consider the extension $k(y_{\xi_1})/k$ given by $y_{\xi_1}^p - y_{\xi_1} = \alpha_1 \neq 0$, the group fixing the extension is not all \mathbb{F}_q and in particular $[k(y_{\xi_1}) : k] = p$. Therefore $[k(\vec{y}_{\vec{\xi}}) : k] = p^m$.

Conversely, in case $[k(\vec{y}_{\vec{\xi}}) : k] = p^m$, necessarily $[k(y_{\xi_1}) : k] = p$ and the argument is reversible and it follows $\vec{\xi}$ is invertible. \square

Corollary 8.7. *The cyclic subextensions of degree p^m are given by $k(\vec{y}_{\vec{\xi}})$ where $\vec{y}_{\vec{\xi}}$ is given by (8.1), where $\vec{\xi}$ is invertible and we have*

$$\vec{y}_{\vec{\xi}}^p \dot{-} \vec{y}_{\vec{\xi}} = \vec{\xi} \dot{\cdot} \vec{\alpha}. \quad \square$$

In particular, taking a basis $\{\vec{\mu}_1, \dots, \vec{\mu}_n\}$ of $W_m(\mathbb{F}_q)$ over $W_m(\mathbb{F}_p)$, we have that $K = k(\vec{y}) = k(\vec{y}_{\vec{\mu}_1}, \dots, \vec{y}_{\vec{\mu}_n})$.

Proposition 8.8. *Let k be a field such that $\mathbb{F}_q \subseteq k$. Let K/k be an abelian extension with Galois group isomorphic to $W_m(\mathbb{F}_q)$. Assume that $K = k(\vec{z}_1, \dots, \vec{z}_n)$ with $\vec{z}_i \in W_m(K)$, $\text{Gal}(k(\vec{z}_i)/k) \cong \mathbb{Z}/p^m\mathbb{Z}$, $1 \leq i \leq n$. Then all the subextensions $k \subseteq k(\vec{z}) \subseteq K$ such that*

$\text{Gal}(k(\vec{z})/k) \cong \mathbb{Z}/p^m\mathbb{Z}$ are given by

$$\vec{z} = \sum_{i=1}^n \vec{\alpha}_i \cdot \vec{z}_i,$$

with $\vec{\alpha}_i \in W_m(\mathbb{F}_p)$, $1 \leq i \leq n$ and some $\vec{\alpha}_{i_0}$ invertible.

Proof. Let $G := \text{Gal}(K/k) = \langle \sigma_1, \dots, \sigma_n \rangle$ such that $\sigma_i \vec{z}_j = \vec{z}_j \dot{+} \vec{\delta}_{ij}$ with $\vec{\delta}_{ij} = \begin{cases} \vec{1} & \text{if } i = j \\ \vec{0} & \text{if } i \neq j \end{cases}$.

Let $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in W_m(\mathbb{F}_p)$ and let $\vec{z} = \sum_{i=1}^n \vec{\alpha}_i \cdot \vec{z}_i$. Let $\wp(\vec{z}_i) = \vec{z}_i^p \dot{-} \vec{z}_i = \vec{\gamma}_i$ with $\vec{\gamma}_i = (\gamma_{i1}, \dots, \gamma_{im})$ and $\gamma_{i1} \notin \wp(k)$. Then

$$\wp(\vec{z}) = \sum_{i=1}^n \vec{\alpha}_i \cdot \wp(\vec{z}_i) = \sum_{i=1}^n \vec{\alpha}_i \cdot \vec{\gamma}_i =: \vec{\gamma},$$

with $\gamma_1 = \sum_{i=1}^n \alpha_{i1} \gamma_{i1}$. We have $[k(\vec{z}) : k] = p^m \iff \gamma_1 \notin \wp(k)$.

Now assume $\wp(\vec{z}) = \sum_{i=1}^n \vec{\alpha}_i \cdot \vec{\gamma}_i = \vec{\gamma} = \wp(\vec{A})$ for some $\vec{A} \in W_m(k)$. Then $\wp(\vec{z} \dot{-} \vec{A}) = \vec{0}$, that is, $\vec{z} \dot{-} \vec{A} \in W_m(\mathbb{F}_p)$, $\vec{z} = \vec{\beta} \dot{+} \vec{A}$ with $\vec{\beta} \in W_m(\mathbb{F}_p)$. In this case, if existed $\vec{\alpha}_{i_0}$ invertible, then $\vec{z} = \sum_{i=1}^n \vec{\alpha}_i \cdot \vec{z}_i = \vec{\beta} \dot{+} \vec{A}$ so that

$$\vec{z}_{i_0} = \sum_{\substack{i=1 \\ i \neq i_0}}^n \vec{\alpha}_{i_0}^{-1} \cdot \vec{\alpha}_i \cdot \vec{z}_i \dot{+} \vec{\alpha}_{i_0}^{-1} \cdot \vec{\beta} \dot{+} \vec{\alpha}_{i_0}^{-1} \cdot \vec{A}.$$

Now, because $\vec{\beta} \in W_m(\mathbb{F}_p) \subseteq W_m(k)$ and $\vec{A} \in W_m(k)$, it follows that $\vec{z}_{i_0} \in k(\vec{z}_1, \dots, \vec{z}_{i_0-1}, \vec{z}_{i_0+1}, \dots, \vec{z}_n)$, that

$$K = k(\vec{z}_1, \dots, \vec{z}_n) = k(\vec{z}_1, \dots, \vec{z}_{i_0-1}, \vec{z}_{i_0+1}, \dots, \vec{z}_n)$$

and that $[K : k] \leq p^{m(n-1)} < p^{mn}$, which is absurd.

In summary, if some $\vec{\alpha}_{i_0}$ were invertible, $\vec{\gamma} = \wp(\vec{z}) \notin \wp(W_m(k))$.

With this procedure we obtain t extensions $k(\vec{z})$ with $[k(\vec{z}) : k] = p^m$ and $t = |\{(\vec{\alpha}_1, \dots, \vec{\alpha}_n) \mid \vec{\alpha}_i \in W_m(\mathbb{F}_p) \text{ and some } \vec{\alpha}_i \text{ invertible}\}|$.

We have $\vec{\alpha}_1, \dots, \vec{\alpha}_n \in W_m(\mathbb{F}_p)$ are non invertible if and only if $\alpha_{11} = \alpha_{21} = \dots = \alpha_{n1} = 0$ where $\vec{\alpha}_i = (\alpha_{i1}, \dots, \alpha_{im})$, $1 \leq i \leq n$. Thus $t = |W_m(\mathbb{F}_p)^n| - |W_{m-1}(\mathbb{F}_p)^n| = p^{nm} - p^{n(m-1)} = q^m - q^{m-1}$.

Now, two of these extensions $k(\vec{z}), k(\vec{w})$ satisfy $k(\vec{z}) = k(\vec{w}) \iff \vec{z} = \vec{j} \cdot \vec{w} \dot{+} \vec{c}$ with $\vec{j} \in W_m(\mathbb{F}_p)$ invertible and $\vec{c} \in W_m(k)$ (Proposition 8.1). Since \vec{z} and \vec{w} are “linear” combinations of $\vec{z}_1, \dots, \vec{z}_n$ over $W_m(\mathbb{F}_p)$, $\vec{c} = \vec{0}$ and $\vec{j} \in W_m(\mathbb{F}_p)^*$. Finally, $|W_m(\mathbb{F}_p)^*| = |W_m(\mathbb{F}_p)| - |W_{m-1}(\mathbb{F}_p)| = p^m - p^{m-1}$.

In this way, we have obtained $\frac{q^m - q^{m-1}}{p^m - p^{m-1}}$ distinct extensions $k(\vec{z})/k$ of degree p^m and therefore all of them. \square

To study how to generate this type of extensions, we have the same result as in Theorem 7.2. Let $K = k(\vec{y})$ be such that $\vec{y}^q \dot{-} \vec{y} = \vec{\alpha}$ and where $\text{Gal}(K/k) \cong W_m(\mathbb{F}_q)$. Let $L = k(\vec{z})$ be such that $\vec{z}^q \dot{-} \vec{z} = \vec{\beta}$. For $\vec{A}_{n-1}, \vec{A}_{n-2}, \dots, \vec{A}_1, \vec{A}_0 \in W_m(\mathbb{F}_q)$ we define $\mathcal{R}(\vec{X}) \in W_m(\mathbb{F}_q)[\vec{X}]$ by

$$\mathcal{R}(\vec{X}) := \vec{A}_{n-1} \cdot \vec{X}^{p^{n-1}} \dot{+} \vec{A}_{n-2} \cdot \vec{X}^{p^{n-2}} \dot{+} \dots \dot{+} \vec{A}_1 \cdot \vec{X}^p \dot{+} \vec{A}_0 \cdot \vec{X}.$$

Theorem 8.9. *With the above notation, we have $k(\vec{y}) = k(\vec{z})$ if and only if (there exist $\vec{A}_{n-1}, \vec{A}_{n-2}, \dots, \vec{A}_1, \vec{A}_0 \in W_m(\mathbb{F}_q)$ satisfying $\mathcal{R}(\vec{\beta}) = 0$ with $\vec{\beta} \in W_m(\mathbb{F}_q) \iff \vec{\beta} = 0$) and $\vec{D} \in W_m(k)$ such that*

$$(8.2) \quad \vec{z} = \mathcal{R}(\vec{y}) \dot{+} \vec{D}.$$

Proof. The proof is analogous to the one of Theorem 7.3 using the formalism of Witt operations. We will give just a few details.

First assume that $k(\vec{y}) = k(\vec{z})$. Let $\sigma_i \in G$ given by $\sigma_i(\vec{y}) = \vec{y} \dot{+} \vec{\mu}_i$, $1 \leq i \leq n$. Let $\vec{w} = \mathcal{R}(\vec{y})$. Then $\sigma \in G$ is given by $\sigma = \sigma_1^{b_1} \dots \sigma_n^{b_n}$ with $b_i \in \mathbb{Z}$, $0 \leq b_i \leq p^m - 1$, $1 \leq i \leq n$. We have $\sigma(\vec{w}) = \vec{w} \dot{+} \mathcal{R}(\sum_{i=1}^n b_i \vec{\mu}_i)$. In particular $\sigma_i(\vec{w}) = \vec{w} \dot{+} \mathcal{R}(\vec{\mu}_i)$.

If $\sigma_i(\vec{z}) = \vec{z} \dot{+} \vec{\xi}_i$, $1 \leq i \leq n$, then $\{\vec{\xi}_1, \dots, \vec{\xi}_n\}$ is a basis of $W_m(\mathbb{F}_q)$ over $W_m(\mathbb{F}_p)$. We want to find $\vec{A}_0, \dots, \vec{A}_{n-1} \in W_m(\mathbb{F}_q)$ such that $\mathcal{R}(\vec{\mu}_i) = \vec{\xi}_i$, $1 \leq i \leq n$.

We have

$$\mathcal{R}(\vec{\mu}_i) = \vec{\xi}_i, 1 \leq i \leq n \iff \vec{M} \cdot \begin{bmatrix} \vec{A}_0 \\ \vec{A}_1 \\ \vdots \\ \vec{A}_{n-2} \\ \vec{A}_{n-1} \end{bmatrix} = \begin{bmatrix} \vec{\xi}_1 \\ \vec{\xi}_2 \\ \vdots \\ \vec{\xi}_{n-1} \\ \vec{\xi}_n \end{bmatrix}$$

where \vec{M} is the matrix

$$\vec{M} = \begin{bmatrix} \vec{\mu}_1 & \vec{\mu}_1^p & \cdots & \vec{\mu}_1^{p^{n-2}} & \vec{\mu}_1^{p^{n-1}} \\ \vec{\mu}_2 & \vec{\mu}_2^p & \cdots & \vec{\mu}_2^{p^{n-2}} & \vec{\mu}_2^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vec{\mu}_{n-1} & \vec{\mu}_{n-1}^p & \cdots & \vec{\mu}_{n-1}^{p^{n-2}} & \vec{\mu}_{n-1}^{p^{n-1}} \\ \vec{\mu}_n & \vec{\mu}_n^p & \cdots & \vec{\mu}_n^{p^{n-2}} & \vec{\mu}_n^{p^{n-1}} \end{bmatrix}.$$

Now, it is clear that $\det \vec{M} = (\det M, \dots)$ where

$$M = \begin{bmatrix} \mu_1 & \mu_1^p & \cdots & \mu_1^{p^{n-2}} & \mu_1^{p^{n-1}} \\ \mu_2 & \mu_2^p & \cdots & \mu_2^{p^{n-2}} & \mu_2^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n-1} & \mu_{n-1}^p & \cdots & \mu_{n-1}^{p^{n-2}} & \mu_{n-1}^{p^{n-1}} \\ \mu_n & \mu_n^p & \cdots & \mu_n^{p^{n-2}} & \mu_n^{p^{n-1}} \end{bmatrix}.$$

We have $\det M \in \mathbb{F}_q^*$ so that $\det \vec{M}$ is a unit of $W_m(\mathbb{F}_q)$ so \vec{M} is invertible. Therefore there exist such $\vec{A}_i \in W_m(\mathbb{F}_q)$ and they are unique satisfying $\sigma(\vec{w}) = \vec{w} \dot{+} \vec{\xi}_i$. The rest of the proof is analogous to that of Theorem 7.3. \square

Now we study the case of rational function fields. Let $k = k_0(T)$ be a rational function field where k_0 is a finite field such that $\mathbb{F}_q \subseteq k_0$. We have the result analogous to that of [3, Theorem 5.5].

Theorem 8.10. *Let K/k be an extension such that $\text{Gal}(K/k) \cong W_m(\mathbb{F}_q)$ and such that $P_1, \dots, P_r \in R_T^+$ and possibly \mathcal{P}_∞ , are the ramified primes. Then $K = k(\vec{y})$ is given by*

$$\vec{y}^q \dot{-} \vec{y} = \vec{\beta} = \vec{\delta}_1 \dot{+} \cdots \dot{+} \vec{\delta}_r \dot{+} \vec{\gamma},$$

with $y_1^q - y_1 = \beta_1$ irreducible, $\delta_{ij} = \frac{Q_{ij}}{P_i^{e_{ij}}}$, $e_{ij} \geq 0$, $Q_{ij} \in R_T$ and if $e_{ij} > 0$, then $e_{ij} = \lambda_{ij} p^{m_{ij}}$, $\gcd(\lambda_{ij}, p) = 1$, $0 \leq m_{ij} < n$, $\gcd(Q_{ij}, P_i) = 1$ and $\deg(Q_{ij}) < \deg(P_i^{e_{ij}})$, and $\gamma_j = f_j(T) \in R_T$ with $\deg f_j = \nu_j p^{m_j}$ and $\gcd(q, \nu_j) = 1$, $0 \leq m_j < n$ when $f_j \notin k_0$.

Proof. For the first reduction of separating the irreducible polynomials in the denominator, we proceed as in [3, Theorem 5.5]. Once we have this simplification, we proceed as Schmid [6, §2, page 162] or [5, §3, page 115], and as in the proof of Theorem 5.3 using Corollary 8.7. \square

To study the decomposition of \mathcal{P}_∞ in a cyclic p -extension, we recall the following result.

Proposition 8.11. *Let K/k be as in Theorem 8.10 with $n = 1$. Let $\gamma_1 = \dots = \gamma_s = 0$, $\gamma_{s+1} \in k_0^*$, $\gamma_{s+1} \notin \wp(k_0)$ and finally, let $t + 1$ be the first index such that $f_{t+1} \notin k_0$ (and therefore $p \nmid \deg f_{t+1}$). Then, the ramification index of \mathcal{P}_∞ is p^{m-t} , the inertia degree of \mathcal{P}_∞ is p^{t-s} and the decomposition number of \mathcal{P}_∞ is p^s . In particular \mathcal{P}_∞ decomposes fully in K/k if and only if $\vec{\gamma} = \vec{0}$.*

Proof. [3, Proposition 5.6]. \square

Remark 8.12. Another equivalent form of Proposition 8.11, is that \mathcal{P}_∞ decomposes fully in K/k if and only if there exists $\vec{\theta} \in W_m(k)$ such that $\vec{\gamma} = \vec{\theta}^p \stackrel{\bullet}{=} \theta = \wp(\theta)$.

From Proposition 8.11 and with a proof analogous to that of Proposition 6.5, we obtain:

Proposition 8.13. *Let K/k be as in Theorem 8.10. If $\vec{\gamma} = \vec{0}$, then \mathcal{P}_∞ decomposes fully. Conversely, if \mathcal{P}_∞ decomposes fully there exists a decomposition as in Theorem 8.10, with $\vec{\gamma} = \vec{0}$.*

Proof. The proof is similar to that of Proposition 6.3. \square

REFERENCES

- [1] Garcia, Arnaldo & Stichtenoth, Henning, *Elementary Abelian p -Extensions of Algebraic Function Fields*, manuscripta math. **72**, 67–79 (1991).
- [2] Hasse, Helmut, *Theorie der relativ zyklischen algebraischen Funktionenkörper*, J. Reine Angew. Math. **172**, 37–54 (1934).
- [3] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Genus Fields of Abelian Extensions of Congruence Rational Function Fields*, Finite Fields Appl. **20**, 40–54 (2013).
- [4] Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel, *Campos ciclotómicos numéricos y de funciones (versión preliminar)*, <http://arxiv.org/abs/1407.3238>.
- [5] Schmid, Hermann Ludwig, *Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p* , J. Reine Angew. Math. **175**, 108–123 (1936).
- [6] Schmid, Hermann Ludwig, *Zur Arithmetik der zyklischen p -Körper*, J. Reine Angew. Math. **176**, 161–167 (1936).
- [7] Villa–Salvador, Gabriel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.
- [8] Witt, Ernst, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n . Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p* , J. Reine Angew. Math. **176**, 126–140 (1936).

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.

E-mail address: jbarreto@ctrl.cinvestav.mx

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO, ACADEMIA DE MATEMÁTICAS. PLANTEL SAN LORENZO TEZONCO, PROLONGACIÓN SAN ISIDRO No. 151, COL. SAN LORENZO, IZTAPALAPA, C.P. 09790, MÉXICO, D.F.

E-mail address: fausto.jarquin@uacm.edu.mx

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.

E-mail address: mrzedowski@ctrl.cinvestav.mx

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.

E-mail address: gvillasalvador@gmail.com, gvilla@ctrl.cinvestav.mx